ROB BONTA
Attorney General of California
ANYA M. BINSACCA, State Bar No. 189613
Supervising Deputy Attorney General
KRISTIN A. LISKA, State Bar No. 315994
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3916
Fax: (415) 703-5480
E-mail: Kristin.Liska@doj.ca.gov
Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

SACRAMENTO DIVISION

CHRISTOPHER KOHLS, et al.,

Plaintiffs,

v.

ROB BONTA, in His Official Capacity as Attorney General of the State of California, and SHIRLEY N. WEBER, in Her Official Capacity as California Secretary of State,

Defendants.

Case No. 2:24-cv-02527-JAM-CKD

DECLARATION OF KRISTIN A. LISKA IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Date:	August 5, 2025
Time:	1:00 p.m.
Dept:	6
Judge:	The Honorable John A. Mendez
Trial Date:	Not Scheduled
Action Filed:	9/17/2024

I, Kristin A. Liska, declare as follows:

1. I am a Deputy Attorney General authorized to practice in this court, and I represent defendants Attorney General Rob Bonta and Secretary of State Shirley N. Weber in this action.

2. Copies of the following legislative history materials can be found online at: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240AB2839.

3. Attached as **Exhibit 1** is a true and correct copy of the April 9, 2024 Assembly Committees on Elections analysis of Assembly Bill 2839 (AB 2839).

4. Attached as **Exhibit 2** is a true and correct copy of the April 26, 2024 Assembly Committee on the Judiciary analysis of AB 2839.

5. Attached as **Exhibit 3** is a true and correct copy of the May 20, 2024 Assembly floor analysis of AB 2839.

6. Attached as **Exhibit 4** is a true and correct copy of the June 14, 2024 Senate Committee on Elections and Constitutional Amendments analysis of AB 2839.

7. Attached as **Exhibit 5** is a true and correct copy of the June 28, 2024 Senate Committee on the Judiciary analysis of AB 2839.

8. Attached as **Exhibit 6** is a true and correct copy of the August 27, 2024 Senate floor analysis of AB 2839.

9. Attached as **Exhibit 7** is a true and correct copy of the August 30, 2024 Assembly floor analysis of AB 2839.

10. Attached as **Exhibit 8** is a true and correct copy of the April 8, 2024 Assembly Committee on Elections analysis of Assembly Bill 2655 (AB 2655).

11. Attached as **Exhibit 9** is a true and correct copy of the April 23, 2024 Assembly Committee on the Judiciary analysis of AB 2655.

12. Attached as **Exhibit 10** is a true and correct copy of the June 15, 2025 Senate Committee on Elections and Constitutional Amendments analysis of AB 2655.

13. Attached as **Exhibit 11** is a true and correct copy of the June 28, 2024 Senate Committee on the Judiciary analysis of AB 2655.

14. Attached as **Exhibit 12** is a true and correct copy of the August 26, 2024 Senate floor analysis of AB 2655.

15. Attached as **Exhibit 13** is a true and correct copy of the August 28, 2024 Assembly floor analysis of AB 2655.

16. Attached as **Exhibit 14** is a true and correct copy of the February 27, 2023 tweet from user Jack Poso with a manipulated video of former President Joe Biden. This tweet can be found at https://x.com/JackPosobiec/status/1630263716473077766 (last accessed March 7, 2025).

17. Attached as **Exhibit 15** is a true and correct copy of Mikael Thalen, *"Legitimate Use of Deepfakes": AI-Generated Video of Biden Declaring World War 3, Bringing Back Draft Splits Experts*, Daily Dot (March 2, 2023), https://www.dailydot.com/debug/biden-deepfake-wwiii/ (last accessed March 7, 2025).

18. Attached as **Exhibit 16** is a true and correct copy of Arijeta Lajka & Philip Marcelo, *Fake AI Images of Putin, Trump Being Arrested Spread Online*, PBS.com (March 23, 2023), https://www.pbs.org/newshour/politics/fake-ai-images-of-putin-trump-being-arrested-spread-online (last accessed March 7, 2025).

19. Attached as **Exhibit 17** is a true and correct copy of Matt Shuham, *DeSantis Campaign Ad Features AI Fakes of Trump Hugging Fauci*, Huffington Post (June 8, 2023), https://www.huffpost.com/entry/desantis-trump-fauci-fake-ai-ad_n_64822436e4b025003edc3c8b (last accessed March 7, 2025).

20. Attached as **Exhibit 18** is a true and correct copy of the press release from the New Hampshire Department of Justice entitled *Steven Kramer Charged With Voter Suppression Over AI-Generated President Biden Robocalls*," dated May 23, 2024 and available at https://www.doj.nh.gov/news-and-media/steven-kramer-charged-voter-suppression-over-ai-generated-president-biden-robocalls (last accessed March 7, 2025).

21. Attached as **Exhibit 19** is a true and correct copy of the press release from the Federal Communications Commission entitled *FCC Proposes $6 Million Fine for Illegal Robocalls that Used Biden Deepfake Generative AI Voice Message*," dated May 23, 2024 and available at

https://www.doj.nh.gov/sites/g/files/ehbemt721/files/inline-documents/sonh/item-2-kramer-robocall-nal.pdf (last accessed March 7, 2024).

22. Attached as **Exhibit 20** is a true and correct copy of X's Help Center article on reporting violations, available at https://help.x.com/en/rules-and-policies/x-report-violation (last accessed March 7, 2025).

23. Attached as **Exhibit 21** is a true and correct copy of an excerpt from Rumble's terms of service addressing reporting content, available in full at https://rumble.com/s/terms (last accessed March 7, 2025).

24. Attached as **Exhibit 22** is a true and correct copy of an excerpt from the Babylon Bee's terms of service addressing reporting content that infringes copyrights, available in full at https://babylonbee.com/terms (last accessed March 7, 2025).

I declare under penalty of perjury under the laws of the State of California that the foregoing is true.

Executed this 7th day of March, 2025, in Daly City, California.

/s/ Kristin A. Liska
KRISTIN A. LISKA
Deputy Attorney General

INDEX OF EXHIBITS

INDEX OF EXHIBITS

EXHIBIT 1

Date of Hearing: April 10, 2024

ASSEMBLY COMMITTEE ON ELECTIONS
Gail Pellerin, Chair
AB 2839 (Pellerin) – As Introduced February 15, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: Elections: deceptive media in advertisements.

SUMMARY: Prohibits the distribution of campaign advertisements and other election communications that contain materially deceptive and digitally altered or created images, audio, and video, except as specified. Allows a court to issue injunctive relief prohibiting the distribution of such content, and to award general or special damages against the person that distributed the content. Specifically, **this bill**:

1) Prohibits a person, committee, or other entity from knowingly distributing an advertisement or other election communication containing materially deceptive and digitally altered or created image or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign, during a specified period of time, if the files are of any of the following:

    a) A candidate portrayed as doing or saying something that the candidate did not do or say.

    b) An officer holding an election or conducting a canvass portrayed as doing or saying something in connection with the election that the officer did not do or say.

    c) An elected official portrayed as doing or saying something in connection with the election that the official did not do or say.

    d) A voting machine, ballot, voting site, or other elections-related property or equipment portrayed in a materially false way.

2) Provides that the prohibition detailed above applies only during the following time periods:

    a) 120 days before any election.

    b) With respect to content depicting an officer holding an election or conducting a canvass and depicting elections equipment and materials, 120 days before any election through 60 days after the election.

3) Permits a candidate, notwithstanding the prohibition detailed above, to portray themself as doing or saying something that the candidate did not do or say if the image or audio or video file includes a disclaimer stating "This (image/video/audio) has been manipulated." Requires this disclaimer to comply with the following:

    a) In the case of visual media, requires the text of the disclaimer to appear in a size that is easily readable, as specified.

b) In the case of a video, requires the disclaimer to appear for the duration of the video.

c) In the case of media that consists of audio only, requires the disclaimer to be read in a manner that can be easily heard by the average listener at both the beginning and the end of the audio. For audio that is longer than two minutes, the disclaimer must also be included during the audio at intervals of not more than two minutes each.

4) Permits a recipient of a materially deceptive and digitally altered or digitally created image or audio or video file distributed in violation of this bill, a candidate or committee participating in the election, or an officer holding an election or conducting a canvass, to seek the following relief:

a) Injunctive or other equitable relief prohibiting the distribution of the materially deceptive file. Requires the court in this case to award a prevailing plaintiff reasonable attorney's fees and costs. Provides that such an action is entitled to precedence in court, as specified.

b) General or special damages against the person, committee, or other entity that distributed that materially deceptive file. Requires the court to award attorney's fees and costs to a prevailing party in such an action.

5) Provides that in any civil action brought under this bill, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

6) Provides that this bill does not apply to any of the following:

a) A radio or television broadcasting station, as specified, when it broadcasts materially deceptive and digitally altered or created content as part of a bona fide news coverage if the broadcast clearly acknowledges that the audio or visual media does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.

b) A regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication, that routinely carries news and commentary of general interest, and that publishes materially deceptive and digitally altered or digitally created content if the publication clearly states that the materially deceptive file does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.

c) Materially deceptive audio or visual media that constitutes satire or parody.

7) Defines the following terms, for the purposes of this bill:

a) "Advertisement" to mean any general or public communication that is authorized or paid for the purpose of supporting or opposing a candidate for elective office or a ballot measure and that is broadcast by or through television, radio, telephone, or text, or disseminated by print media, including billboards, video billboards or screens, and other similar types of advertising.

b) "Election communication" to mean any general or public communication not covered under "advertisement" that is broadcast by or through television, radio, telephone, or text, or disseminated by print media, including billboards, video billboards or screens, and other similar types of communications, that concerns any of the following:

   i) A candidate for office or ballot measure.

   ii) Voting or refraining from voting in an election.

   iii) The canvass of the vote.

c) "Materially deceptive and digitally modified or created image or audio or video file" to mean an image or audio or video file that has been intentionally manipulated in a manner such that all of the following conditions are met:

   i) The file is the product of digital manipulation, artificial intelligence (AI), or machine learning, including deep learning techniques, that merges, combines, replaces, or superimposes content onto an image or an audio or video file, creating an image or an audio or video file that appears authentic, or generates an inauthentic image or an audio or video file that appears authentic.

   ii) The file represents a false portrayal of a candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, or other elections property or equipment. Provides that "a false portrayal of the candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, or other elections property or equipment" means the file would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the file than if the person were hearing or seeing the unaltered, original version of the file.

   iii) The person, committee, or other entity distributed the file knowing the portrayal of the candidate, elected official, elections official, or elections materials, property, or equipment was false or with a reckless disregard for the true portrayal of the candidate, the elected official, the elections official, or the elections materials, property, or equipment. Provides that this provision is presumed when a file has been intentionally manipulated to represent a false portrayal, but may be rebutted.

8) Provides that a file that contains only minor modifications that do not lead to significant changes to the perceived contents or meaning of the content is not a "materially deceptive and digitally modified or created image or audio or video file" for the purposes of this bill, as specified.

9) Contains various findings and declarations and contains a severability clause.

EXISTING STATE LAW:

1) Prohibits a person, committee, or other entity, until January 1, 2027, from distributing with actual malice, within 60 days of an election at which a candidate for elective office will

appear on the ballot, materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

a) Defines "materially deceptive audio or visual media," for these purposes, as an image or an audio or visual recording of a candidate's appearance, speech or conduct that has been intentionally manipulated in a manner that both of the following are true about the image or audio or video recording:

   i) It would falsely appear to a reasonable person to be authentic; and,

   ii) It would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than the person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.

b) Provides that this prohibition does not apply if the audio or visual media includes a disclaimer stating "This (image/video/audio) has been manipulated," and the disclaimer complies with specified requirements.

c) Permits a candidate whose voice or likeness appears in deceptive audio or visual media distributed in violation of this provision to seek the following relief:

   i) Injunctive or other equitable relief prohibiting the distribution of the materially deceptive audio or visual media in violation of this bill. Provides that such an action is entitled to precedence in court, as specified.

   ii) General or special damages against the person, committee, or other entity that distributed that audio or visual media. Permits the court to award reasonable attorney's fees and costs to a prevailing party in such an action.

d) Provides that in any civil action brought pursuant to these provisions, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

e) Provides that this prohibition shall not be construed to alter or negate any rights, obligations, or immunities of an interactive service provider under Section 230 of the federal Communications Decency Act.

f) Provides that this prohibition does not apply to any of the following:

   i) A radio or television broadcasting station, as specified, in either of the following circumstances:

      (1) When it broadcasts materially deceptive audio or visual media as part of a bona fide newscast, news interview, news documentary, or on-the-spot coverage of bona fide news events, if the broadcast clearly acknowledges through content or disclosure that there are questions about the authenticity of the audio or visual

media, as specified.

(2) When it is paid to broadcast materially deceptive audio or visual media.

ii) An internet website, or a regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication, that routinely carries news and commentary of general interest, and that publishes materially deceptive audio or visual media covered by this prohibition, if the publication clearly states that the media does not accurately represent the speech or conduct of the candidate.

iii) Materially deceptive audio or visual media that constitute satire or parody. (Elections Code §20010, as amended by Section 3 of Chapter 745 of the Statutes of 2022)

2) Prohibits a person, firm, association, corporation, campaign committee, or organization, beginning January 1, 2027, with actual malice, from producing, distributing, publishing, or broadcasting campaign material, as defined, that contains either of the following types of pictures or photographs, as specified, unless the campaign material includes a disclaimer that the picture is not an accurate representation of fact:

a) A picture or photograph of a person or persons into which the image of a candidate for public office is superimposed.

b) A picture or photograph of a candidate for public office into which the image of another person or persons is superimposed. (Elections Code §20010, as amended by Section 4 of Chapter 745 of the Statutes of 2022)

EXISTING FEDERAL LAW provides, pursuant to Section 230 of the federal Communications Decency Act, that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. §230)

FISCAL EFFECT: None. This bill is keyed non-fiscal by the Legislative Counsel.

COMMENTS:

1) **Author's Amendments**: After the committee's deadline for pre-committee author's amendments, the author proposed the following minor and technical amendments to this bill:

a) Add the following to the findings and declarations included in the bill:

The labeling information required by this bill is narrowly tailored to provide consumers with factual information about the inauthenticity of particular images, audio, video, or text content in order to prevent consumer deception.

b) Amend the language on page 3, lines 19-25 of the bill, to make technical corrections:

(b) (1) A person, committee, or other entity shall not, during the time period set forth in

subdivision (c), with the intent to influence an election or solicit funds for a candidate or campaign, knowingly distribute an advertisement or other election communication containing **a** materially deceptive and digitally altered or digitally created ~~**images**~~ **image** or audio or video files of any the following:

c) Amend the language on page 4, lines 25-27 as follows to correct a drafting error:

(2) For ~~**elections officials**~~ **people** and items set forth in subparagraphs (B) and ~~**(C)**~~ **(D)** of paragraph (1) of subdivision (b), 120 days before any election through 60 days after the election, inclusive.

d) Amend the language to add "an officer holding an election or conducting a canvass" to the list of entities that can bring an action to enforce this bill.

This analysis reflects those proposed author's amendments.

2) **Purpose of the Bill**: According to the author:

> Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content, in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections.
>
> Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls.

3) **Threats of Manipulated Media in Campaign Communications**: The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. In 1850, the First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chapter 38, Statutes of 1850). California law today includes various provisions criminalizing deceptive tactics that undermine election integrity or interfere with voters' ability to participate in elections. This includes laws that prohibit distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur (Elections Code §18302); prohibit the misleading use of government seals in campaign literature (Elections Code §18304); and prohibit coercing or deceiving people into voting in a way that was inconsistent with the person's intent (Elections Code §§18573, 18573.5).

Advancements in technology have made it increasingly simple to produce false and misleading media that closely resembles authentic content. Moreover, platforms like social media have facilitated the rapid dissemination of deceptive media to large audiences at

minimal cost. Given these developments, the potential threat posed by manipulated media to future elections' integrity may be more significant than in the past.

As described in greater detail below, past legislative efforts have addressed concerns about manipulated media's use to deceive voters during elections. Those laws, however, are limited, and are designed primarily to target the harms to *candidates* that may result from the distribution of manipulated media of those candidates. In contrast, this bill aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. Additionally, this bill targets media that portrays elections materials and equipment in materially deceptive ways. The author and supporters of this bill believe that these provisions will safeguard voters against deceitful media that could undermine trust in the electoral process.

4) **Recent Examples of Materially Deceptive Campaign Communications**: As evidence of the need for this bill, the author points to the following incidents, as reported in the media:

- Elections in Bangladesh were recently plagued by a number of deepfake videos promoting disinformation and intended to influence the election results.

- During elections in Slovakia, deepfake audio was released of a conversation discussing how to rig the election. Due to a media blackout and social media policies, debunking the audio proved difficult.

- A political action committee in support of candidate Ron DeSantis released a political advertisement with a deepfake of former President Donald Trump, and DeSantis' campaign released an advertisement featuring AI generated images of former President Trump and Dr. Anthony Fauci. Neither included disclaimers that they were manipulated content.

- In New Hampshire's 2024 Presidential Primary, an AI generated deepfake audio of President Biden was used as part of a robocall to dissuade voters from voting in the primary.

5) **Previous Legislation Related to Materially Deceptive Media in Campaigns**: In 2019, in response to concerns that deepfake technology could be used to spread misinformation in political campaigns, the Legislature approved and Governor Newsom signed AB 730 (Berman), Chapter 493, Statutes of 2019. Deepfake technology refers to software capable of producing a realistic looking video of someone saying or doing something that they did not, in fact, say or do. This technology has advanced rapidly in recent years thanks to the use of AI to help train the software.

AB 730 prohibits the distribution of materially deceptive audio or visual media with actual malice with the intent to injure a candidate's reputation or to deceive a voter into voting for or against a candidate, unless the materially deceptive audio or visual media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, but rather applies to any intentional manipulation of audio or visual images that results in a version that a reasonable observer would believe to be authentic. Nonetheless, the increasing

availability and advancing capability of deepfake technology was the immediate impetus for that bill.

AB 730 was designed as an update to California's "Truth in Political Advertising Act," a law enacted in 1998 (through the passage of AB 1233 (Leach), Chapter 718, Statutes of 1998) that prohibited campaign material that contains a picture of a person into which a candidate's image is superimposed, or contains a picture of a candidate into which another person's image is superimposed, except if a specified disclaimer was included. The Truth in Political Advertising Act was introduced in response to the use of photoshopped pictures in campaign materials, and accordingly was designed to target the manipulation of photographs in campaign materials. In the 20 years following its passage, however, it was never amended to update the law to address more modern techniques of manipulating campaign materials in a manner that can mislead voters. AB 730 replaced the Truth in Political Advertising Act with a law that regulates not only altered photographs in campaign materials, but also audio and video media that have been altered in a materially deceptive manner.

AB 730 included a January 1, 2023 sunset date. In 2022, however, the Legislature approved AB 972 (Berman), Chapter 745, Statutes of 2022, which extended the sunset date to January 1, 2027. AB 972 did not otherwise change the provisions of AB 730. If the current January 1, 2027 sunset date is not repealed or extended, the original Truth in Political Advertising Act as enacted by AB 1233 of 1998 would go back into effect.

Because the impetus for AB 730 was concern about the potential that people might create deepfake media appearing to be accurate representations of the conduct of candidates for office, its provisions apply exclusively to images or audio or video recordings of a candidate's appearance, speech, or conduct. Relatedly, candidates for elective office who are the target of materially deceptive media are the only entities that can seek injunctive relief or damages under AB 730. Materially deceptive images, audio, or video that appear in campaign communications are not covered by AB 730 if that media is not of a candidate. For instance, if a candidate digitally manipulated video or a photo of a campaign rally to make the crowd look significantly larger than it actually was, such manipulation would not be covered by AB 730 as long as the manipulated image or video was not materially deceptive about a candidate's appearance, speech, or conduct. Similarly, manipulated and materially deceptive content in advertisements related to ballot measures, or in communications that seek to undermine confidence in the electoral process but that do not mention candidates directly, generally would not be covered by AB 730.

6) **Free Speech Considerations**: The First Amendment to the United States (US) Constitution, which also applies to states under the Fourteenth Amendment, provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

This bill seeks to regulate the distribution of media containing intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised

about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds, then, likely would hinge on whether the court found this bill's provisions to be narrowly tailored.

This bill includes provisions to limit its scope to communications posing the greatest threat to election integrity. It applies only to communications that include media that was intentionally manipulated to be materially deceptive. To be "materially deceptive," a communication would have to "cause a reasonable person to have a fundamentally different understanding or impression of the expressive content" of the media; minor and cosmetic changes alone would not be considered to be materially deceptive. Furthermore, liability under this bill requires knowledge of the media's false portrayal of a candidate, elections official, elected official, or elections materials or equipment, or action with reckless disregard for the true portrayal of the candidate, official, or materials or equipment. Moreover, this bill applies only to communications intended "to influence an election or solicit funds for a candidate or campaign."

This bill's application is restricted to deceptive portrayals of candidates or elections officials in the 120 days before an election to target periods where a deceptive communication would be more likely to harm election integrity. (For communications that include deceptive portrayals of elections officials or election materials and equipment, the bill additionally applies in the 60 days after the election. This post-election period is intended to protect against deceptive communications that could undermine confidence in the integrity of recently-conducted elections during the period when election results are being finalized and newly-elected officials are taking office.) Finally, relief under this bill requires the plaintiff to establish a violation through clear and convincing evidence.

Whether these limitations adequately protect this bill from a potential constitutional challenge is a question that falls more squarely within the jurisdiction of the Assembly Judiciary Committee, where this bill will be heard next if it is approved by this committee. However, while these limitations may help protect the bill against a constitutional challenge, they may also make it harder for the bill to achieve its aims of limiting the spread of materially deceptive communications that have the potential to undermine election integrity.

7) **Digital Alterations Only**: While digital tools may have made it considerably easier and less costly to create and distribute convincingly-realistic but materially deceptive elections-related communications, the harm that this bill presumably seeks to address is the fact that those communications were created or altered to be deceptive, and not the fact that the

creation or alteration was done using digital means. To the extent that someone is able to create convincingly-realistic and materially deceptive communications without using digital means, it seems that those communications would pose an equal threat to elections as a communication that was digitally created or altered. The author and the committee may wish to consider whether limiting this bill to *digitally* created or altered media is necessary.

8) **Arguments in Support**: The sponsor of this bill, the California Initiative for Technology & Democracy, a Project of California Common Cause, writes in support:

> Current California law requires disclosure that content has been manipulated for certain deepfakes of a candidate, to better inform voters on the credibility of the content they are consuming. However, this disclosure requirement only applies in a very narrow set of circumstances with a high burden of proof, and only applies to media portraying candidates… [F]or the most pernicious disinformation in our elections, we must do more than require disclosures -- we must prevent it from even entering the information ecosystem to truly protect the integrity of our democracy…
>
> In order to help ensure California elections are free and fair, AB 2839 would prevent the use of the most potentially harmful offline deepfakes close to an election… AB 2839 would address significant deficiencies of current law by removing potential disinformation from the information ecosystem and expanding coverage to additional key election-related subjects beyond just candidates. In short, AB 2839 ensures deepfake-free campaigning close to Election Day, when voter attention is highest.

9) **Arguments in Opposition**: In opposition to this bill, the Electronic Frontier Foundation writes:

> We respectfully oppose your bill A.B. 2839, which not only bans the distribution of materially deceptive or altered content in relation to an election, but also places burdens on those unconnected to the creation of the content but who distribute it (internet websites, newspapers, etc.) regardless of whether they know of the prohibited manipulation. We recognize the complex issues raised by potentially harmful artificially generated election content. However, this bill's "exceptions" for only some types of republishers, and by requiring them to publish a disclaimer, does not reflect the full First Amendment protection due the republication of speech pertaining to matters of public interest by those not connected with the creation of the offending material.
>
> The First Amendment requires this distinction between those who create synthetic media and those not directly involved in it. The Fourth Circuit relied on this distinction in striking down a Maryland law that extended the reach of campaign finance law to include 'online platforms,' thus imposing disclosure requirements on them when they ran online ads. AB 2389, as written, suffers from the same constitutional defect.

10) **Related Legislation**: AB 2355 (Wendy Carrillo), which is also being heard in this committee today, requires a political advertisement that is generated in whole or in part using AI to include a disclaimer stating that fact.

    AB 2655 (Berman), which is also being heard in this committee today, requires large online platforms to block the posting or sending of materially deceptive and digitally modified or created content related to elections, during specified periods before and after an election.

11) **Double-Referral**: This bill has been double-referred to the Assembly Judiciary Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

California Initiative for Technology & Democracy, a Project of California Common Cause (Sponsor)
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
California Chamber of Commerce (if amended)
Campaign Legal Center
Computer and Communications Industry Association (if amended)
Courage California
Disability Rights California
Software & Information Industry Association (if amended)
TechNet (if amended)
Verified Voting
Voices for Progress Education Fund

Opposition

Chamber of Progress (unless amended)
Electronic Frontier Foundation

Analysis Prepared by: Ethan Jones / ELECTIONS / (916) 319-2094

EXHIBIT 2

Date of Hearing: April 30, 2024

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
AB 2839 (Pellerin) – As Amended April 11, 2024

As Proposed to be Amended

SUBJECT: ELECTIONS: DECEPTIVE MEDIA IN ADVERTISEMENTS

KEY ISSUE: SHOULD CALIFORNIA PROHIBIT THE DISTRIBUTION OF CAMPAIGN ADVERTISEMENTS THAT CONTAIN MATERIALLY DECEPTIVE AND FAKE IMAGES, AUDIO, AND VIDEO?

SYNOPSIS

Artificial intelligence technology presents a myriad of opportunities to better humanity. From predictive analytics in healthcare settings, to making workplaces more efficient, to making travel safer for all Americans, the benefits of artificial intelligence seem endless. However, there is a dark side to these technological advancements. Artificial intelligence can now produce lifelike, yet fake, images, video, and audio. Particularly troubling these fake images, video, and audio can be manipulated to influence American elections by portraying candidates as saying things they did not, impugning the credibility of election officials, and generally undermining public faith in the electoral process.

This bill seeks to protect the integrity of California's electoral process by prohibiting the distribution of campaign advertisements and other election communications that contain materially deceptive and digitally altered or created images, audio, and video within specified time periods surrounding an election. The measure would limit the prohibition to content that was intentionally manipulated then disseminated by a person who knew it was false or recklessly ignored the veracity of the content. The bill exempts from its prohibitions media companies who republish the content, so long as the republication is conducted in a limited manner and subject to various disclaimers. The measure also clarifies that the prohibition only applies 120 days in advance of an election and concludes 60 days after Election Day.

This bill is sponsored by the California Initiative for Technology & Democracy and is supported by a coalition of labor, legal aid and environmental organizations. The proponents of this bill highlight the growing use of and threat posed by disinformation related to elections. They note that fake content developed utilizing artificial technology can generate exceedingly lifelike content that average users may not be able to deem fake. This measure is opposed by the Electronic Frontier Foundation who question the measure's constitutionality, especially provisions related to the republication of content. This measure was previously heard and approved by the Committee on Elections by a vote of 6-1.

SUMMARY: Prohibits the distribution of campaign advertisements and other election communications that contain materially deceptive and digitally altered or created images, audio, and video within specified time periods surrounding an election. Specifically, **this bill**:

1) Prohibits a person, committee, or other entity from knowingly distributing, with the intent to influence an election or solicit funds for a candidate or campaign, an advertisement or other

election communication containing a materially deceptive and digitally altered or digitally created image or audio or video file of any of the following:

a) A candidate portrayed as doing or saying something that the candidate did not do or say;

b) An officer holding an election or conducting a canvass portrayed as doing or saying something in connection with the election that the officer holding an election or conducting a canvass did not do or say;

c) An elected official portrayed as doing or saying something in connection with the election that the elected official did not do or say; or

d) A voting machine, ballot, voting site, or other elections-related property or equipment portrayed in a materially false way.

2) Provides, notwithstanding the prohibition in 1), a candidate may portray themselves as doing or saying something that the candidate did not do or say, but only if the image or audio or video file includes a disclosure stating "This ____ has been manipulated." and complies with the following requirements:

a) The blank in the disclosure states whether or not the media is an image, audio, or video;

b) For visual media the text of the disclosure is in a size that is easily readable by the average viewer and no smaller than the largest font size of other text appearing in the visual media, as specified; and

c) For media that consists of audio only, the disclosure must read in a clearly spoken manner and in a pitch that can be easily heard by the average listener, at the beginning of the audio, at the end of the audio, or in two minute intervals, as specified.

3) Provides that the prohibition in 1) only applies during the following time periods:

a) One hundred twenty days before any election; and

b) Sixty days after the election, as specified.

4) Authorizes the recipient of a materially deceptive and digitally altered or digitally created image or audio or video file distributed in violation of this, as well as a candidate or committee participating in the election, or officer holding an election or conducting a canvass to seek injunctive or other equitable relief prohibiting the distribution of the materially deceptive and digitally altered or digitally created image or audio or video file.

5) Provides that in addition to the injunctive or equitable relief provided in 4) a plaintiff may also seek general or special damages against the person, committee, or other entity that distributed the materially deceptive and digitally altered or digitally created image or audio or video file in violation of this bill.

6) Provides that a prevailing party in an action brought pursuant to 4) or 5) is entitled to reasonable attorney's fees and costs.

7) Provides that in any action brought pursuant to 4) or 5) the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

8) Provides that this bill does not apply to a radio or television broadcasting station, including a cable or satellite television operator, programmer, or producer, that broadcasts any materially deceptive and digitally altered or digitally created image or audio or video file prohibited by this bill as part of a bona fide newscast, news interview, news documentary, or on-the-spot coverage of bona fide news events, if the broadcast clearly acknowledges through content or a disclosure, in a manner that can be easily heard or read by the average listener or viewer, that the materially deceptive audio or visual media does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.

9) Provides that this bill not apply to a regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication, that routinely carries news and commentary of general interest, and that publishes any materially deceptive and digitally altered or digitally created image or audio or video file prohibited by this bill, if the publication clearly states that the materially deceptive and digitally altered or digitally created image or audio or video file does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.

10) Defines "advertisement" to mean any general or public communication that is authorized or paid for the purpose of supporting or opposing a candidate for elective office or a ballot measure and that is broadcast by or through television, radio, telephone, or text, or disseminated by print media, including billboards, video billboards or screens, and other similar types of advertising.

11) Defines "artificial intelligence" to mean an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

12) Defines "committee" to mean any person or combination thereof who does any of the following:

    a) Receives contributions totaling two thousand dollars ($2,000) or more in a calendar year;

    b) Makes independent expenditures totaling one thousand dollars ($1,000) or more in a calendar year; or

    c) Makes contributions totaling ten thousand dollars ($10,000) or more in a calendar year to or at the behest of candidates or committees.

13) Defines "election communication" to mean any general or public communication not covered under "advertisement" that is broadcast by or through television, radio, telephone, or text, or disseminated by print media, including billboards, video billboards or screens, and other similar types of communications, that concerns any of the following:

    a) A candidate for office or ballot measure;

    b) Voting or refraining from voting in an election;

c) The canvass of the vote.

14) Defines "materially deceptive and digitally modified or created image or audio or video file" to mean an image or an audio or video file that has been intentionally manipulated in a manner such that all of the following conditions are met:

a) The image or audio or video file is the product of digital manipulation, artificial intelligence, that appears authentic, but contains a false portrayal of specified actors or items; and

b) The person, committee, or other entity distributed the image or audio or video file knowing the portrayal of the candidate for elective office, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment was false or with a reckless disregard for the true portrayal of the candidate, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment.

15) Provides that "materially deceptive and digitally modified or created image or audio or video file" does not include any image or audio or video file that contains only minor modifications that do not lead to significant changes to the perceived contents or meaning of the content, as specified.

16) Defines for the purpose of 14) a "false portrayal of the candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, or other elections property or equipment" to mean the image or audio or video file would cause a reasonable person to believe that the content is authentic and to have a fundamentally different understanding or impression of the expressive content of the image or audio or video file than that person would have if the person were hearing or seeing the authentic version of the image or audio or video file.

17) Defines "officers holding an election or conducting a canvass" to include, but be not limited to, the Secretary of State as the chief elections officer, and their staff, as it relates to performance of any of their duties related to administering the provisions of the Elections Code, and elections officials and their staff, including temporary workers and poll workers, and members of a precinct board, in their performance of any duty related to assisting with holding an election or conducting a canvass.

18) Defines "recipient" to include a person who views, hears, or otherwise perceives an image or audio or video file that was initially distributed in violation of this bill.

19) Provides that the provisions of this bill apply regardless of the language in which the advertisement or solicitation was provided.

20) Provides that actions to enforce this bill are to be placed on a judicial calendar in the order of their date of filing and are to be given precedence.

21) Adopts numerous findings and declarations about election security, the state's compelling interest in election security, and that this measure is narrowly tailored to achieve the state's interest.

22) Adopts a severability clause.

EXISTING LAW:

1) Prohibits, until January 1, 2027, a person, committee, or other entity from distributing, with actual malice, materially deceptive audio or visual media of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate, within 60 days of an election in which the candidate will appear on the ballot. (Elections Code Section 20010 (a).)

2) Exempts from the prohibition of 1) any audio or visual media that includes a disclosure stating: "This _____ has been manipulated." (Elections Code Section 20010 (b).)

3) Authorizes a candidate for office who's voice of likeness was utilized in violation of 1) to seek injunctive or other equitable relief prohibiting the distribution of audio or visual media in violation. (Elections Code Section 20010 (c)(1).)

4) Defines for the purpose of 1), "materially deceptive audio or visual media" to mean an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:

   a) The image or audio or video recording would falsely appear to a reasonable person to be authentic; and

   b) The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording. (Elections Code Section 20010 (e).)

5) Exempts from the prohibition of 1) audio or visual media that constitutes satire or parody. (Elections Code Section 20010 (d).)

6) Prohibits a candidate or committee on their behalf from representing, in connection with an election campaign, either orally or in campaign material, that the candidate has the support of a committee or organization that includes as part of its name the name or any variation upon the name of a qualified political party with which the candidate is not affiliated, together with the words "county committee," "central committee," "county," or any other term that might tend to mislead the voters into believing that the candidate has the support of that party's county central committee or state central committee, when that is not the case. (Elections Code Section 20007.)

7) Requires any paid political advertisement that refers to an election or to any candidate for state or local elective office and that is contained in or distributed with a newspaper, to bear on each surface or page thereof, in type or lettering at least half as large as the type or lettering of the advertisement or in 10-point roman type, whichever is larger, the words "Paid Political Advertisement." (Elections Code Section 20008.)

8) Provides that any person who in any manner interferes with the officers holding an election or conducting a canvass, as to prevent the election or canvass from being fairly held and

lawfully conducted, or with the voters lawfully exercising their rights of voting at an election, is punishable by imprisonment for 16 months or two or three years. (Elections Code Section 18502.)

9) Prohibits the following conduct within 100 feet of the entrance to a building that contains a polling place or an outdoor site, including a curbside voting area, at which a voter may cast or drop off a ballot:

   a) Soliciting a vote or speaking to a voter on the subject of marking the voter's ballot;

   b) Placing a sign relating to voters' qualifications or speak to a voter on the subject of the voter's qualifications, except as specified;

   c) Photographing, video recording, or otherwise recording a voter entering or exiting a polling place; or

   d) Obstructing ingress, egress, or parking. (Elections Code Section 18541.)

FISCAL EFFECT: As currently in print this bill is keyed non-fiscal.

COMMENTS: As more Americans turn away from traditional news sources, the market for online election-related content is growing. Unfortunately, without traditional media outlets serving as gatekeepers of information, the amount of blatantly false or misleading election-related content appearing on the internet is growing significantly. Given American's propensity to dabble in conspiracy theories and take at face value information provided on the internet, this fake election-related content can have profound and troubling impacts on our democracy. Seeking to protect California voters from the proliferation of fake election content, this bill would prohibit the distribution of campaign advertisements and other election communications that contain materially deceptive and digitally altered or created images, audio, and video within specified time periods surrounding an election. In support of this measure, the author states:

> Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections.
>
> Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls.

The risk of false information in electioneering is as old as American democracy. The use of questionable tactics to win an election are as old as America's democracy. The election of 1800 between John Adams and Thomas Jefferson features a panoply of disgusting and unfounded attacks traded between the two candidates. Indeed, paraphrasing the actual terms used by each side, Jefferson's camp accused Adams of being a woman while Adams camp accused Jefferson of being non-white. (Kerwin Stewart, *Founding Fathers' dirty campaign*, CNN (2008) available at: https://www.cnn.com/2008/LIVING/wayoflife/08/22/mf.campaign.slurs.slogans/.) Indeed, some of the handbills containing these attacks were so believable it is reported that America's

first First Lady, Martha Washington, once said of Jefferson that he was, "one of the most detestable of mankind." (*Ibid*.) As technology has improved so have the attacks and the tactics used to disseminate campaign-related falsehoods.

In the highly contested election of 1876 between Rutherford B. Hayes and Samuel J. Tilden, campaign operatives worked with friendly newspapers to accuse each side of "stealing" the election. (Ronald G. Shafer, *The ugliest presidential election in history: Fraud, voter intimidation and a backroom deal*, The Washington Post (Nov. 24, 2020) available at: https://www.washingtonpost.com/history/2020/11/24/rutherford-hayes-fraud-election-trump/.) The television era made spreading falsehoods much easier. It's been determined that in the contentious election of 1960, President Kennedy knowingly spread falsehoods about the state of America's missile deterrence systems. (Daniel Bush, *The history of lies on the campaign trail*, PBS Newshour (Dec. 4, 2015) available at: https://www.pbs.org/newshour/politics/the-history-of-lies-on-the-campaign-trail.) Notoriously, Richard Nixon utilized television and attacks on the press to hide his involvement in the Watergate break-in in the lead up to the 1972 Presidential campaign. (*Ibid*.) Perhaps most confounding of all of the historic election mistruths broadcast by candidates, Gerald Ford, at the height of the Cold War, once tried to contend that the Soviet Union did not have significant influence in Eastern Europe in a bid to "win" a televised debate with Jimmy Carter. (*Ibid.*)

With the social media-driven misinformation campaign surrounding the 2016 election, and the outright lies about the integrity of the 2020 election, fear about the use of technology to manipulate elections is growing and legitimate. In fact, signs of manipulation are already evidence in the 2024 Presidential election. During the recent New Hampshire Presidential Primary, one study suggested that between 5,000 and 20,000 New Hampshire residents received artificially generated phone calls, impersonating President Biden, that told them not to vote in the state's primary. (Adam Edelman, *States turn their attention to regulating AI and deepfakes as 2024 kicks off*, NBC News, (Jan. 22, 2024) available at: www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122.) As the United States faces an incredibly contentious rematch between President Joe Biden and Donald Trump, one can only imagine that the threat of fake online content designed to influence the election will grow.

California's historic efforts to maintain election integrity. Dating back to California's founding, state law has sought to protect election integrity. The First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chap. 38, Stats. 1850). Modern election law recognizes the myriad of tools parties can utilize to impact elections. State law already prohibits the distribution or dissemination of misleading information about election logistics including polling places and the date of elections. Additionally, the law prohibits misusing government seals on election information, coercing peoples vote, electioneering within a set distance of polling places, maliciously distributing fake election materials.

This bill recognizes the significant threat that emerging technologies and misinformation pose to the integrity of future elections. To that end, this bill prohibits the distribution of campaign advertisements and other election communications that contain materially deceptive and digitally altered or created images, audio, and video 120 days before and 60 days after an election. The bill generally limits the prohibition to the distribution of fake video, audio, or imagines of candidates, election officials, elected officials, or election machinery, as specified. Most notably,

the bill is limited only to false election information that is disseminated in the form of materially deceptive and digitally modified or created image or audio or video files. This term is defined as, "a file that is intentionally manipulated in a manner such that a reasonable person would believe the image, video, or audio to be authentic and that the information was distributed with the knowledge of the files inaccuracy or reckless disregard for the truth underlying the accuracy of the image, video, or audio files." The measure, generally, exempts from the prohibition of this bill news media that republish the false content for the purpose of a newsworthy story on the false image, video or audio. Finally, the measure adopts numerous definitions and makes various findings and declarations.

By limiting the dissemination of speech related to elections, this measure implicates the First Amendment and the broad protections it provides to political speech. By prohibiting the dissemination of false election information this measure represents a government-imposed restriction on speech, thus implicating the First Amendment to the United States Constitution. The First Amendment provides that "Congress shall make no law . . . prohibiting the freedom of speech." As interpreted by the courts and incorporated against the states by the due process clause of the 14th Amendment, the First Amendment prevents any government entity (not just Congress) from enacting any law or adopting any policy that burdens freedom of speech. In addition, Article I, Section 2 of the California Constitution guarantees to every person the freedom to "speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right." Moreover, the First Amendment not only protects the right to speak, as a logical corollary it protects the "right to receive information and ideas." (*Stanley v Georgia* (1969) 394 U.S. 557, 564.)

This bill implicates both the right to speak about elections, as well as the right to receive information regarding them. Furthermore, given that this bill implicates political speech, it is almost certainly going to be subject to the most exacting legal review afforded to restrictions on speech. Indeed, the First Amendment affords the "broadest protection" to the "discussion of public issues" and "political expression in order to assure the unfettered interchange of ideas for the bringing about of political and social changes desired by the people." (*McIntyre v Ohio Election Commission* (1997) 514 U.S. 334.) It is difficult to imagine any content more related to "political expression" and "discussion of public issues" than content about candidates and elections. Notably, however, the Supreme Court has also held that there is "no constitutional value in false statements of fact." (*Gertz v. Robert Welch, Inc*. (1974) 418 U.S. 323.) Nonetheless, while false statements have little constitutional value, the modern Supreme Court has argued that the remedy for false speech is more true speech, and false speech tends to call forth true speech. (*United States v Alvarez* (2012) 567 U.S. 709.)

This bill firmly falls somewhere in this constitutional spectrum. Looking at the case law, it is clear that this measure, as a prior restriction on speech, would be subject to strict scrutiny. (See, e.g. *Frisby v. Schultz* (1988) 487 U.S. 474.) To overcome this level of scrutiny, the government must demonstrate that it has a *compelling interest* in regulating the speech and its restrictions are *narrowly tailored* to meet that goal. It would appear obvious, especially in light of the fact that California has regulated the integrity of elections since its inception, that the government has a compelling interest in protecting election integrity. Thus, it must be determined whether this bill is sufficiently narrowly tailored. Proponents of this bill argue that this measure is narrowly tailored in that its prohibitions are limited to 120 days prior to and 60 days after an election. Further, the proponents note that the bill specifically targets artificially doctored images, audio, and video of specific figures integral to the election process. They argue, for example, that any

person would still be free to post a video of themselves speaking falsehoods about candidates so long as the video were not altered in any way. Furthermore, the proponents of this bill note that it mirrors the holding in *New York Times v. Sullivan*, which authorized some prior restraints.

When examining this bill in light of the *New York Times v. Sullivan* holding, several key aspects of that decision are notable. First, the court held that, "even a false statement may be deemed to make a valuable contribution to public debate, since it brings about 'the clearer perception and livelier impression of truth, produced by its collision with error.'" (*New York Times Co. v. Sullivan* (1964) 376 U.S. 254, 279 *internal citations omitted.*) However, that decision also provided fewer speech protections to falsehoods, even those about public officials, made with *actual malice*. (*Ibid.*) The proponents of this measure contend that it meets the *New York Times v. Sullivan* standard because it is limited only to false statements that are intentionally made, "knowing the portrayal of the candidate for elective office, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment was false or with a reckless disregard for the true portrayal of the candidate, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment." Finally, it should be noted that the enforcement provisions of this bill adopt a "clear and convincing evidence" standard which is a higher standard of proof than typically applies to civil actions like the one proposed by this measure.

The constitutional questions posed by this bill present an exceedingly difficult decision for this Committee. It does appear that the prohibitions proposed by this bill, at least as applied to the original content creator, are as narrowly tailored as possible and certainly implicate a compelling government interest. Furthermore, the adoption of the malice-like intent standard further narrows the bill. However, the Committee cannot ignore the longstanding preference of the courts to protect all forms of speech. Moreover, the current Supreme Court has demonstrated a willingness to greatly expand the scope of speech rights, especially when the speaker's views align with the court's majority. (See, e.g. *Citizens United v. Federal Election Commission* (2010) 558 U.S. 310.) Thus, while this bill is certainly designed to provide the greatest chance of withstanding constitutional review, it is almost guaranteed to be the subject of litigation.

Proposed amendments seek to make this bill as narrowly tailored as possible. As noted above, this measure will almost certainly be the target of immediate litigation should it be signed into law. Seeking to further buttress this measure, to bring terminology into alignment with other bills involving artificial intelligence technology, and clarify various terms, the author is proposing several amendments. First, the author wishes to make findings to indicate that this bill is designed to be as narrowly tailored as possible. Those amendments would amend the findings section of the bill to read:

> (4) In order to ensure California elections are free and fair, California must, for a limited time before and after elections, prevent the use of deepfakes and disinformation meant to prevent voters from voting and deceive voters based on fraudulent content. ***The provisions of this bill are narrowly tailored to advance California's compelling interest in protecting free and fair elections.***

It should be noted that while these findings are helpful, a court is not compelled to following the Legislature's judgment on this matter.

Secondly, the author proposes to further refine the definition of "materially deceptive and digitally modified or created image or audio or video file." Accordingly, that rather lengthy and detailed definition will now read:

> "Materially deceptive and digitally modified or created image or audio or video file" means an image or an audio or video file that has been intentionally manipulated in a manner such that all of the following conditions are met:
>
> (i) The image or audio or video file is the product of digital manipulation, artificial intelligence, ~~**or machine learning, including deep learning techniques, that merges, combines, replaces, or superimposes content onto an image or an audio or video file, creating an image or an audio or video**~~ file that appears authentic, ***that appears authentic, but contains a false portrayal of any of the following:***
> ***(I)A candidate for elective office,***
> ***(II) An elected official,***
> ***(III) Elections official,***
> ***(IV) Voting machine,***
> ***(V) Ballots,***
> ***(VI) Voting sites,***
> ***(VII) Other property or equipment related to an election, or elections process***. ~~**or generates an inauthentic image or an audio or video file that appears authentic.**~~
> ~~**(ii) (I) The image or audio or video file represents a false portrayal of a candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, or other elections property or equipment.**~~
> ***(ii)*** ~~**(II)**~~ For the purposes of this clause, "a false portrayal of the candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, or other elections property or equipment" means the image or audio or video file would cause a reasonable person ***to believe that the content is authentic and*** to have a fundamentally different understanding or impression of the expressive content of the image or audio or video file than that person would have if the person were hearing or seeing the ***authentic*** ~~**unaltered, original**~~ version of the image or audio or video file.
> (iii) The person, committee, or other entity distributed the image or audio or video file knowing the portrayal of the candidate for elective office, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment was false or with a reckless disregard for the true portrayal of the candidate, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment. This clause is presumed when an image or audio or video file has been intentionally manipulated to represent a false portrayal of the candidate for elective office, the elected official, the elections official, or the voting machine, ballot, voting site, or other elections property or equipment, but may be rebutted.

Finally, in consultation with the Committee on Privacy and Consumer Protection, the author is proposing to add the Privacy Committee's new standard definition of artificial intelligence to this bill to promote consistency in the codes. That definition will now read:

> ***(2) "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.***

Additional policy considerations. Should this measure advance, the author and the proponents may wish to consider three additional policy considerations. First, in opposition to this measure the Electronic Frontier Foundation objects to the restriction on media outlets republishing the false information. *The author may wish to consider working with the opposition to see if this section can be further narrowed or refined* to avoid potential litigation and further defend the bill against First Amendment scrutiny. Secondly, the bill applies to false images, audio, and video of elected officials, candidates, and election officials but omits *former* elected officials. Thus, for example, should an artificially generated video of former President Barack Obama speaking poorly of his Vice President, now-President Joe Biden, be created it would not be covered by this measure. While this omission would arguably expand a bill seeking to be as narrowly tailored as possible, it may be a worthwhile type of false speech to regulate. Finally, the author may wish to consider expanding the 60-day post-election timeline. For example, the 2024 election is set for Tuesday November 5, 2024. Should Congress meet on January 6, 2025 to certify the election that date would be *outside* the 60-day window. Thus, a bad actor would have several days to flood the internet with artificially generated content related to the election. Furthermore, the President will not be inaugurated until January 20, 2025. The author may wish to consider expanding the post-election prohibitions until all elected officials are sworn into office.

ARGUMENTS IN SUPPORT*:* This bill is sponsored by the California Initiative for Technology & Democracy and is supported by a coalition of labor, legal aid and environmental organizations. In support of this bill the California Initiative for Technology & Democracy writes:

> California is entering its first-ever generative artificial intelligence (AI) election, in which disinformation powered by generative AI and social media will pollute our information ecosystems like never before. In a few clicks, bad actors such as conspiracy theorists, foreign states, online trolls, and unscrupulous campaigns have the power to create false images, video, and audio to deceive and manipulate voters.
>
> These deepfakes could include depictions of a candidate accepting a bribe, a fake video of an elections official "caught on tape" saying that voting machines are not secure, or an artificial robocall in the Governor's voice incorrectly telling millions of Californians their voting site has changed. The technology is widely available, provided for little to no cost, and rapidly improving in its ability to produce realistic deepfakes. This AI-fueled disinformation can skew specific election results by deceiving voters or impacting voter turnout, call results into question, and more generally undermine faith in our elections, their security, and democratic systems.
>
> This problem is not a hypothetical future but a real and present danger to democracy. Generative AI has been used in various ways – most of them deeply deceptive – to influence national elections in Slovakia, Bangladesh, Argentina, Pakistan, and elsewhere, including in our own country. In New Hampshire's 2024 presidential primary election, an AI-generated deepfake robocall of President Biden was used to dissuade voters from voting in the primary. Just this month, a supporter of former President Trump created a deepfake image depicting Trump with Black Americans, trying to influence Black voters to support Trump.
>
> In order to help ensure California elections are free and fair, AB 2839 would prevent the use of the most potentially harmful offline deepfakes close to an election. Specifically, the bill would ban the distribution of specified digitally generated or manipulated communications

that portray a candidate, an elected official, or elections official as doing or saying something that they did not do or say, or specified election equipment and voting sites in a materially false way, within 120 days before an election and, for those regarding election officials or voting systems, within 60 days after the election through offline means such as robocalls, mailers, television advertisements. AB 2839 would address significant deficiencies of current law by removing potential disinformation from the information ecosystem and expanding coverage to additional key election-related subjects beyond just candidates. In short, AB 2839 ensures deepfake-free campaigning close to Election Day, when voter attention is highest.

***ARGUMENTS IN OPPOSITION**:* This measure is opposed by the Electronic Frontier Foundation. They note:

> We respectfully oppose A.B. 2839, which not only bans the distribution of materially deceptive or altered content in relation to an election, but also places burdens on those unconnected to the creation of the content but who distribute it (internet websites, newspapers, etc.) regardless of whether they know of the prohibited manipulation. We recognize the complex issues raised by potentially harmful artificially generated election content. However, this bill's "exceptions" for only some types of republishers, and by requiring them to publish a disclaimer, does not reflect the full First Amendment protection due the republication of speech pertaining to matters of public interest by those not connected with the creation of the offending material.
>
> The First Amendment requires this distinction between those who create synthetic media and those not directly involved in it. The Fourth Circuit relied on this distinction in striking down a Maryland law that extended the reach of campaign finance law to include 'online platforms,' thus imposing disclosure requirements on them when they ran online ads.12 AB 2389, as written, suffers from the same constitutional defect.
>
> By extending beyond the direct publishers of the content and toward re-publishers, A.B. 2839 burdens and holding liable re-publishers of content in a manner that has been found unconstitutional. For these reason, we must oppose A.B. 2839.

REGISTERED SUPPORT / OPPOSITION:

Support

AFSCME AFL-CIO
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
Bay Rising
California Clean Money Campaign
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Campaign Legal Center
Chinese Progressive Association
Courage California
Disability Rights California
Hmong Innovating Politics
Indivisible CA Statestrong

Inland Empire United
League of Women Voters of California
NextGen California
Partnership for The Advancement of New Americans
SEIU California
TechEquity Collaborative
The Partnership for The Advancement of New Americans
Verified Voting
Voices for Progress Education Fund

Support If Amended

California Chamber of Commerce
Computer and Communications Industry Association
Software & Information Industry Association
TechNet

Oppose

Electronic Frontier Foundation

Analysis Prepared by: Nicholas Liedtke / JUD. / (916) 319-2334

EXHIBIT 3

ASSEMBLY THIRD READING
AB 2839 (Pellerin and Berman)
As Amended May 2, 2024
Majority vote

SUMMARY

Prohibits the distribution of campaign advertisements and other election communications that contain media that has been digitally altered in a deceptive way, except as specified. Allows a court to issue injunctive relief prohibiting the distribution of such content, and to award general or special damages against the person that distributed the content.

Major Provisions

1) Prohibits a person, committee, or other entity from knowingly distributing a campaign advertisement or other election communication containing materially deceptive and digitally altered or created image or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign, during a specified period of time, if the files are of any of the following:

   a) A candidate portrayed as doing or saying something that the candidate did not do or say.

   b) An officer holding an election or conducting a canvass portrayed as doing or saying something in connection with the election that the officer did not do or say.

   c) An elected official portrayed as doing or saying something in connection with the election that the official did not do or say.

   d) A voting machine, ballot, voting site, or other elections-related property or equipment portrayed in a materially false way.

2) Provides that the prohibition detailed above applies 120 days before any election and, with respect to content depicting an officer holding an election or conducting a canvass and depicting elections equipment and materials, during the 60 days after the election.

3) Permits a candidate, notwithstanding the prohibition detailed above, to portray themself as doing or saying something that the candidate did not do or say if the media includes a disclaimer, as specified, stating "This (image/video/audio) has been manipulated."

4) Permits a recipient of a communication with deceptively-altered media distributed in violation of this bill, a candidate or committee participating in the election, or an officer holding an election or conducting a canvass, to seek the following relief:

   a) Injunctive or other equitable relief prohibiting the distribution of the media. Requires the court to award a prevailing plaintiff attorney's fees and costs, and provides that such an action is entitled to precedence in court, as specified.

   b) General or special damages against the entity that distributed that deceptively-altered media. Requires the court to award attorney's fees and costs to a prevailing party.

5) Provides that in any civil action brought under this bill, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

6) Provides that this bill does not apply to any of the following:

   a) A broadcasting station or a regularly-published news periodical that distributes deceptively-altered media if the media includes a clear acknowledgement that it is not accurately representative.

   b) Deceptively-altered media that is satire or parody.

7) Provides that deceptively-altered media is subject to the restrictions of this bill if the media has been intentionally manipulated in a manner such that both of the following are true:

   a) The file is the product of digital manipulation or artificial intelligence (AI) that appears authentic, but that contains a false portrayal of a candidate for elective office, an elected official, an elections official, a voting machine, a ballot, a voting site, or other elections property or equipment, as specified.

   b) The entity distributed the file knowing the portrayal was false or with a reckless disregard for the true portrayal, as specified.

COMMENTS

The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. In 1850, the First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chapter 38, Statutes of 1850).

Advancements in technology have made it increasingly simple to produce false and misleading media that closely resembles authentic content. Moreover, platforms like social media have facilitated the rapid dissemination of deceptive media to large audiences at minimal cost. Given these developments, the potential threat posed by manipulated media to future elections' integrity may be more significant than in the past.

Past legislative efforts have addressed concerns about manipulated media's use to deceive voters during elections. Those laws, however, are limited, and are designed primarily to target the harms to *candidates* that may result from the distribution of manipulated media of those candidates. In contrast, this bill aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. Additionally, this bill targets media that portrays elections materials and equipment in materially deceptive ways. The author and supporters of this bill believe that these provisions will safeguard voters against deceitful media that could undermine trust in the electoral process.

A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the United States (US) and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the

restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds, then, likely would hinge on whether the court found this bill's provisions to be narrowly tailored.

This bill includes provisions to limit its scope to communications posing the greatest threat to election integrity in an effort to tailor its provisions. It applies only to communications that include media that was intentionally manipulated to be materially deceptive. Minor and cosmetic changes alone would not be considered to be materially deceptive. Furthermore, liability under this bill requires knowledge of the media's false portrayal of a candidate, elections official, elected official, or elections materials or equipment, or action with reckless disregard for the true portrayal of the candidate, official, or materials or equipment. Moreover, this bill applies only to communications intended "to influence an election or solicit funds for a candidate or campaign."

Whether these limitations adequately protect this bill from a potential constitutional challenge is unclear. However, while these limitations may help protect the bill against a constitutional challenge, they may also make it harder for the bill to achieve its aims of limiting the spread of materially deceptive communications that have the potential to undermine election integrity.

AB 2355 (Wendy Carrillo), which is pending on the Assembly Floor, requires any political advertisement, as specified, that is generated or substantially altered using AI, to include a disclaimer stating that fact.

AB 2655 (Berman), which is pending on the Assembly Floor, requires large online platforms, as defined, to block the posting or sending of materially deceptive and digitally modified or created content related to elections, or to label that content, during specified periods before and after an election.

Please see the policy committee analysis for a full discussion of this bill

According to the Author
"Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content, in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections. Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls."

Arguments in Support
The sponsor of this bill, the California Initiative for Technology & Democracy, a Project of California Common Cause, writes in support, "Current California law requires disclosure that content has been manipulated for certain deepfakes of a candidate, to better inform voters on the credibility of the content they are consuming. However, this disclosure requirement only applies

in a very narrow set of circumstances with a high burden of proof, and only applies to media portraying candidates…In order to help ensure California elections are free and fair, AB 2839 would prevent the use of the most potentially harmful offline deepfakes close to an election… AB 2839 would address significant deficiencies of current law by removing potential disinformation from the information ecosystem and expanding coverage to additional key election-related subjects beyond just candidates. In short, AB 2839 ensures deepfake-free campaigning close to Election Day, when voter attention is highest."

Arguments in Opposition
In opposition to this bill, the Electronic Frontier Foundation writes, "We respectfully oppose… A.B. 2839, which not only bans the distribution of materially deceptive or altered content in relation to an election, but also places burdens on those unconnected to the creation of the content but who distribute it (internet websites, newspapers, etc.) regardless of whether they know of the prohibited manipulation. We recognize the complex issues raised by potentially harmful artificially generated election content. However, this bill's 'exceptions' for only some types of republishers, and by requiring them to publish a disclaimer, does not reflect the full First Amendment protection due the republication of speech pertaining to matters of public interest by those not connected with the creation of the offending material. The First Amendment requires this distinction between those who create synthetic media and those not directly involved in it. The Fourth Circuit relied on this distinction in striking down a Maryland law that extended the reach of campaign finance law to include 'online platforms,' thus imposing disclosure requirements on them when they ran online ads. AB 2389, as written, suffers from the same constitutional defect."

FISCAL COMMENTS

According to the Assembly Appropriations Committee, by authorizing a claim by a recipient of a prohibited communication, a candidate or committee participating in the election, or an officer holding the election or conducting a canvass to enjoin distribution of a prohibited communication and seek damages, this bill may result in an increased number of civil actions that also receive precedence when filed in court, resulting in potentially significant cost pressures of an unknown amount to the courts (Trial Court Trust Fund (TCTF)). It is unclear how many new actions may be filed statewide, but disinformation and hostility regarding elections has grown in recent years and one hour of court time is estimated to cost $1,000 in workload. Although courts are not funded on the basis of workload, increased pressure on staff and the TCTF may create a need for increased court funding from the General Fund (GF) to perform existing duties. The Governor's proposed 2024-25 state budget includes $83.1 million ongoing GF to backfill declining TCTF revenue.

According to the Legislative Analyst's Office, the GF faces a structural deficit in the tens of billions of dollars over the next several fiscal years.

VOTES

ASM ELECTIONS: 6-1-1
YES: Pellerin, Bennett, Berman, Cervantes, Low, Weber
NO: Essayli
ABS, ABST OR NV: Lackey

ASM JUDICIARY: 8-2-2
YES: Kalra, Bryan, Connolly, Haney, Maienschein, McKinnor, Pacheco, Reyes
NO: Essayli, Sanchez
ABS, ABST OR NV: Dixon, Bauer-Kahan

ASM APPROPRIATIONS: 11-3-1
YES: Wicks, Arambula, Bryan, Calderon, Wendy Carrillo, Mike Fong, Grayson, Haney, Hart, Pellerin, Villapudua
NO: Sanchez, Jim Patterson, Ta
ABS, ABST OR NV: Dixon

UPDATED

VERSION: May 2, 2024

CONSULTANT: Ethan Jones / ELECTIONS / (916) 319-2094 FN: 0003170

EXHIBIT 4

SENATE COMMITTEE ON ELECTIONS AND CONSTITUTIONAL AMENDMENTS

Senator Catherine Blakespear, Chair
2023 - 2024 Regular

Bill No:	AB 2839	**Hearing Date:**	6/18/24
Author:	Pellerin		
Version:	5/2/24		
Urgency:	No	**Fiscal:**	No
Consultant:	Scott Matsumoto		

Subject: Elections: deceptive media in advertisements

DIGEST

This bill prohibits the distribution of campaign advertisements and other election communications that contain media that has been digitally altered in a deceptive way. This bill also allows a court to issue injunctive relief prohibiting the distribution of such content, and to award general or special damages against the person that distributed the content.

ANALYSIS

Existing law:

1) Prohibits anyone from, until January 1, 2027, distributing within 60 days of an election materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

2) Prohibits anyone from, beginning January 1, 2027, producing, distributing, publishing, or broadcasting campaign material that contains a superimposed image of a candidate unless the campaign material includes a disclaimer that the picture is not an accurate representation of fact.

This bill:

1) Prohibits anyone from knowingly distributing a campaign advertisement or other election communication containing materially deceptive and digitally altered or created images or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign, during a specified period of time, if:

   a) A candidate is portrayed as doing or saying something they did not do or say;

   b) An officer holding an election or conducting a canvass is portrayed as doing or saying something in connection with the election they did not do or say;

   c) An elected official is portrayed as doing or saying something in connection with the election they did not do or say; or

d) A voting machine, ballot, voting site, or other elections-related property or equipment is portrayed in a materially false way.

2) Provides the prohibition detailed above applies 120 days before any election and, with respect to content depicting an officer holding an election or conducting a canvass and depicting elections equipment and materials, for 60 days after the election.

3) Permits a candidate, notwithstanding the prohibition detailed above, to portray themselves as doing or saying something they did not do or say if the media includes a disclaimer stating "This (image/video/audio) has been manipulated."

4) Permits a recipient of a communication with deceptively-altered media distributed in violation of this bill, a candidate or committee participating in the election, or an elections official, to seek:

a) Injunctive or other equitable relief prohibiting the distribution of the media. Requires the court to award a prevailing plaintiff attorney's fees and costs, and provides such an action is entitled to precedence in court.

b) General or special damages against the entity that distributed the deceptively-altered media. Requires the court to award attorney's fees and costs to a prevailing party.

5) Provides that in any civil action brought under this bill, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

6) Provides this bill does not apply to:

a) A broadcast station or a regularly-published news periodical that distributes deceptively-altered media if the media includes a clear acknowledgement it is not accurately representative; or

b) Deceptively-altered media that is satire or parody.

7) Provides deceptively-altered media is subject to the restrictions of this bill if the media has been intentionally manipulated in a manner such that:

a) The file is the product of digital manipulation or artificial intelligence (AI) that appears authentic, but that contains a false portrayal of a candidate, an elected official, an elections official, a voting machine, a ballot, a voting site, or other elections property or equipment; and

b) The entity distributed the file knowing the portrayal was false or with a reckless disregard for the true portrayal.

BACKGROUND

Manipulated Media in Campaign Communications. The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon.

Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. The inaugural 1850 session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for."

California law today includes various provisions criminalizing deceptive tactics that undermine election integrity or interfere with voters' ability to participate in elections. This includes laws that prohibit distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur; prohibit the misleading use of government seals in campaign literature; and prohibit coercing or deceiving people into voting in a way that was inconsistent with the person's intent.

Artificial Intelligence and Elections. On June 4, 2024, the Senate Committee on Elections and Constitutional Amendments and the Assembly Committee on Elections held a joint information hearing focusing on AI and elections.

The purpose of the hearing was to inform and assist the Legislature in making informed decisions on legislation related to AI-generated and altered content. It became evident that the ease with which people can create and spread mis- and disinformation creates a world where many people may have trouble determining what is fact and what is fiction. The development of increasingly advanced AI tools has made once time-consuming activities much easier to complete, while also enabling the completion of tasks that are otherwise too complex for humans to tackle alone.

State Action. In 2018, the Legislature approved and Governor Brown signed AB 3075 (Berman), Chapter 241, Statutes of 2018 to establish the Office of Elections Cybersecurity (OEC) in the Secretary of State's (SOS) office. The OEC has two primary missions. First, it is responsible for coordinating efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation.

In 2019, the Legislature approved and Governor Newsom signed AB 730 (Berman), Chapter 493, Statutes of 2019. AB 730 sought to address concerns that deepfake technology could be used to spread misinformation in political campaigns. Legislative analyses of AB 730 described "deepfake technology" as software capable of producing a realistic looking video of someone saying or doing something they did not actually say or do.

AB 730 prohibits anyone from distributing deceptive audio or visual media with actual malice and the intent to injure a candidate's reputation or to deceive a voter, unless the media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, it also applies to any intentional manipulation of audio or

visual images where a reasonable person would be misled into believing it was authentic. Notably, AB 730 focused on materially deceptive representations of candidates, and not on deceptive media of other aspects of the electoral process.

AB 730 included a January 1, 2023, sunset date, but in 2022 the Legislature approved AB 972 (Berman), Chapter 745, Statutes of 2022, to extend the sunset date to January 1, 2027.

Tech Accord to Combat Deceptive Use of AI in 2024. In February 2024, 20 technology companies signed the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections." This set of commitments seeks to combat harmful AI-generated content meant to deceive voters. The signatories included Adobe, Amazon, Anthropic, Arm, ElevenLabs, Google, IBM, Inflection AI, LinkedIn, McAfee, Meta, Microsoft, Nota, OpenAI, Snap Inc., Stability AI, TikTok, Trend Micro, Truepic, and X.

The signatories committed to taking the following steps through this year:

1) Develop and implement technology to mitigate risks related to deceptive AI content.
2) Assess and better understand the risks presented by deceptive AI election content.
3) Seek ways to detect the distribution of deceptive AI election content.
4) Seek to address deceptive AI election content.
5) Share best practices and explore pathways to share tools throughout the industry.
6) Provide transparency to the public.
7) Continue to engage with stakeholders to better understand the global risk landscape.
8) Support efforts to raise public awareness regarding deceptive AI election content.

Other States. According to the National Conference of State Legislatures, 16 states (Alabama, Arizona, California, Colorado, Florida, Idaho, Indiana, Michigan, Minnesota, Mississippi, New Mexico, Oregon, Texas, Utah, Washington, and Wisconsin) enacted legislation designed to address deceptive media, including but not limited to, AI.

COMMENTS

1) According to the Author: "Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections.

   "Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls."

2) First Amendment Considerations. The First Amendment to the United States (US) Constitution provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

   This bill seeks to regulate the distribution of intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

   This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds would likely hinge on whether the court found this bill's provisions to be narrowly tailored.

3) Banned Sometimes. This bill prohibits anyone from knowingly distributing a campaign advertisement or other election communication containing materially deceptive and digitally altered or created images or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign from 120 days before an election and, in some cases, 60 days after an election.

   However, for the other six to eight months of the year, such content would be permitted to be provided to the public.

   The Committee may wish to consider whether this distinction is appropriate and why, if content is materially deceptive, the content shouldn't be banned entirely from the platform, regardless of how close to an election such content is posted or displayed.

   AB 2655 (Berman), which is also on the Committee's agenda, requires materially deceptive content posted outside of the same elections-related window covered by this bill to be labeled.

4) Should It Be Okay For Candidates To Create Misleading Content About Themselves? This bill permits a candidate to falsely portray themselves as doing or saying something they did not do or say, as long as the media includes a disclaimer stating "This (image/video/audio) has been manipulated."

   For example, this provision could permit a candidate to use AI to falsely tell voters they voted one way on a measure when they actually voted another way or be portrayed as visiting a location in an effort to appeal to a certain group of voters, when in reality they have never been to that location.

As such, the Committee may wish to consider if there is the potential for candidates to abuse this section of the bill and whether it should be removed.

5) Election Timing. This bill prohibits anyone from knowingly distributing digitally deceptive and altered campaign communication beginning 120 days before an election and ending as many as 60 days after the election. As drafted, this would include any election in California. As a result, in counties where there are large numbers of elections (statewide, legislative, and congressional elections are held in every even-numbered year and many cities hold local elections in odd-numbered years), committees and media companies may be monitoring content almost constantly in order to ensure compliance with the provisions of this bill.

6) Double Referral. If approved by this committee, AB 2839 will be referred to the Committee on Judiciary for further consideration.

RELATED/PRIOR LEGISLATION

AB 2355 (W. Carrillo) of 2024 requires a campaign committee that creates, originally publishes, or originally distributes a political advertisement to include a disclosure stating that the audio, image, or video was generated or substantially altered using AI. AB 2355 is being considered by this committee.

AB 2655 (Berman) of 2024 requires large online social media platforms to block the posting or sending of materially deceptive and digitally modified or created content related to elections, or to label that content, before and after an election. AB 2655 is being considered by this committee.

PRIOR ACTION

Assembly Floor:	59 - 4
Assembly Appropriations Committee:	11 - 3
Assembly Elections Committee:	6 - 1

POSITIONS

Sponsor: California Initiative for Technology and Democracy

Support: American Federation of State, County, and Municipal Employees, AFL-CIO
Bay Rising
Campaign Legal Center
Catalyst California
Center for Countering Digital Hate
Chinese Progressive Association
City and County of San Francisco Board of Supervisors
Disability Rights California
Hmong Innovating Politics
Indivisible CA: Statestrong
League of Women Voters of California

MOVE (Mobilize, Organize, Vote, Empower) the Valley
NextGen CA
Northern California Recycling Association
Partnership for the Advancement of New Americans
SEIU California
TechEquity Action
Young People's Alliance

Oppose: California Broadcasters Association
DIRECT TV, LLC
DISH Network
Electronic Frontier Foundation

-- END --

EXHIBIT 5

SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 2839 (Pellerin)
Version: June 24, 2024
Hearing Date: July 2, 2024
Fiscal: No
Urgency: No
CK

SUBJECT

Elections: deceptive media in advertisements

DIGEST

This bill prohibits a person, committee, or other entity from knowingly distributing an advertisement or other election communication that contains materially deceptive content, as defined and specified, with malice, except as provided, within 120 days of a California election, and in specified cases, 60 days thereafter.

EXECUTIVE SUMMARY

Certain forms of media – audio recordings, video recordings, and still images – can be powerful evidence of what truly took place. While such media have always been susceptible to some degree of manipulation, until recently, fakes were relatively easy to detect. The rapid advancement of AI technology, specifically the wide-scale introduction of generative AI models, has made it drastically cheaper and easier to produce synthetic content – audio, images, text, and video recordings that are not real, but that are so realistic that they are virtually impossible to distinguish from authentic content, including so-called "deepfakes." In the context of election campaigns, such deepfakes can be weaponized to deceive voters into thinking that a candidate said or did something which the candidate did not. A series of bills currently pending before this Committee attempt to address these issues. In an attempt to prevent deepfakes and other materially deceptive content from altering elections, this bill prohibits the knowing distribution, with malice, of advertisements containing material deceptive content of specified material, including specified portrayals of candidates, elections officials, and elections property or equipment.

Supporters of the bill include the League of Women Voters of California and the California Broadcasters Association. It is opposed by several groups, including the Electronic Frontier Foundation and the Motion Picture Association. The bill passed out of the Senate Elections and Constitutional Amendments Committee on a 6 to 0 vote.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides that "Congress shall make no law… abridging the freedom of speech..." (U.S. Const., amend. 1.)

2) Applies the First Amendment to the states through operation of the Fourteenth Amendment. (*Gitlow v. New York* (1925) 268 U.S. 652; *NAACP v. Alabama* (1925) 357 U.S. 449.)

3) Provides that no provider or user of an interactive computer service shall be treated for liability purposes as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230.)

4) Defines "materially deceptive audio or visual media" as an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:
    a. The image or audio or video recording would falsely appear to a reasonable person to be authentic.
    b. The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording. (Elec. Code § 20010(e).)

5) Prohibits a person, committee, or other entity from distributing with actual malice materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate within 60 days of an election at which a candidate for elective office will appear on the ballot, unless specified conditions are met. (Elec. Code § 20010(a).)

6) Exempts audio or visual media that includes a disclosure stating: "This _____ has been manipulated." Requires the blank in the disclosure to be filled with a term that most accurately describes the media, as specified. Requires the following disclosures for visual and audio-only media:
    a. For visual media, the text of the disclosure shall appear in a size that is easily readable by the average viewer and no smaller than the largest font size of other text appearing in the visual media. If the visual media does not include any other text, then the disclosure shall appear in a size that is

easily readable by the average viewer. Requires, for visual media that is video, the disclosure to be displayed throughout the duration of the video.

b. For audio-only media, the disclosure shall be read in the clearly spoken manner and in a pitch that can be easily heard by the average listener, at the beginning of the audio, at the end of the audio, and, if the audio is greater than two minutes in length, interspersed within the audio at intervals of not greater than two minutes each. (Elec. Code § 20010(b).)

7) Permits a candidate for elective office whose voice or likeness appears in a materially deceptive audio or visual media distributed in violation of the above provisions, to seek injunctive or other equitable relief prohibiting the distribution of the audio or visual media in violation. (Elec. Code § 20010(c)(1).)

8) Permits a candidate for elective office whose voice or likeness appears in materially deceptive audio or visual media distributed in violation of the provisions of this bill to bring an action for general or special damages against the person, committee, or other entity that distributed the materially deceptive audio or visual media, as specified. Requires the plaintiff to bear the burden of establishing the violation through clear and convincing evidence in any civil action alleging a violation, as specified. (Elec. Code § 21101(c)(2).)

This bill:

1) Prohibits a person, committee, or other entity, during the time period of 120 days before an election to, in some specified instances, 60 days after the election in California from knowingly distributing, with malice, an advertisement or other election communication containing materially deceptive content of any of the following:
   a) A candidate for any federal, state, or local elected office in California portrayed as doing or saying something that the candidate did not do or say if the content is reasonably likely to harm the reputation or electoral prospects of a candidate.
   b) An elections official portrayed as doing or saying something in connection with an election in California that the elections official did not do or say if the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.
   c) An elected official portrayed as doing or saying something in connection with an election in California that the elected official did not do or say if the content is reasonably likely to harm the reputation or electoral prospects of a candidate or is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.
   d) A voting machine, ballot, voting site, or other property or equipment related to an election in California portrayed in a materially false way if

the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

2) Authorizes, notwithstanding the above, a candidate to portray themself as doing or saying something that the candidate did not do or say, if the content includes a disclosure stating "This [category of content] has been manipulated." and complies with the following requirements:
    a) For visual media, the text of the disclosure shall appear in a size that is easily readable by the average viewer and no smaller than the largest font size of other text appearing in the visual media. If the visual media does not include any other text, the disclosure shall appear in a size that is easily readable by the average viewer. For visual media that is video, the disclosure shall appear for the duration of the video.
    b) If the media consists of audio only, the disclosure shall be read in a clearly spoken manner and in a pitch that can be easily heard by the average listener, at the beginning of the audio, at the end of the audio, and, if the audio is greater than two minutes in length, interspersed within the audio at intervals of not greater than two minutes each.

3) Authorizes a recipient of materially deceptive content distributed in violation hereof, a candidate or committee participating in the election, or an elections official to seek injunctive or other equitable relief prohibiting the distribution of the violative content. The court shall also award a prevailing plaintiff reasonable attorney's fees and costs. Such an action is entitled to precedence in accordance with Section 35 of the Code of Civil Procedure. The bill further authorizes such parties to bring an action for general or special damages against the person, committee, or other entity that distributed the materially deceptive content in violation hereof. The court shall also award a prevailing party reasonable attorney's fees and costs.

4) Requires plaintiffs in the actions outlined above to establish violations by clear and convincing evidence.

5) Provides a list of exemptions from these provisions, including satire or parody, news publications, and a radio or television broadcasting station when it is paid to broadcast materially deceptive content or when it is broadcasting the content as part of a news program and the content is acknowledged to be materially deceptive.

6) Defines the relevant terms, including:

    a) "Advertisement" means any general or public communication that is authorized or paid for the purpose of supporting or opposing a candidate for elective office in California or a ballot measure that appears on a

California ballot and that is broadcast by or through television, radio, telephone, or text, or disseminated by print media, including billboards, video billboards or screens, and other similar types of advertising.

b) "Deepfake" means audio or visual media that is digitally created or modified such that it would falsely appear to a reasonable person to be an authentic record of the actual speech or conduct of the individual depicted in the media.
c) "Malice" means the person, committee, or other entity distributed the audio or visual media knowing the materially deceptive content was false or with a reckless disregard for the truth.
d) "Materially deceptive content" means audio or visual media that is intentionally digitally created or modified, which includes deepfakes, such that the content would falsely appear to a reasonable person to be an authentic record of the content depicted in the media.

7) Requires actions brought pursuant hereto to be placed on the court calendar in the order of their date of filing and to be given precedence.

8) Includes findings and declarations and a severability clause.

COMMENTS

1. Blurring reality: AI-generated content

Generative AI is a type of artificial intelligence that can create new content, including text, images, code, or music, by learning from existing data. Generative AI models can produce realistic and novel artifacts that resemble the data they were trained on, but do not copy it. For example, generative AI can write a poem, draw a picture, or compose a song based on a given prompt or theme. Generative AI enables users to quickly generate new content based on a variety of inputs. Generative AI models use neural networks to identify the patterns and structures within existing data to generate new and original content.

The world has been in awe of the powers of this generative AI since the widespread introduction of AI systems such as ChatGPT. However, the capabilities of these advanced systems leads to a blurring between reality and fiction. The Brookings Institution lays out the issue:

> Over the last year, generative AI tools have made the jump from research prototype to commercial product. Generative AI models like OpenAI's ChatGPT and Google's Gemini can now generate realistic text and images that are often indistinguishable from human-authored content, with generative AI for audio and video not far behind. Given these advances, it's no longer surprising to see AI-generated images of public figures go

> viral or AI-generated reviews and comments on digital platforms. As such, generative AI models are raising concerns about the credibility of digital content and the ease of producing harmful content going forward.
>
> Against the backdrop of such technological advances, civil society and policymakers have taken increasing interest in ways to distinguish AI-generated content from human-authored content.[1]

One expert at the Copenhagen Institute for Future Studies estimates that should large generative-AI models run amok, up to 99 percent of the internet's content could be AI-generated by 2025 to 2030.[2] The problematic applications are seemingly infinite, whether it be deepfakes to blackmail or shame victims, false impersonations to commit fraud, or other nefarious purposes. Infamously, in January of this year, Taylor Swift was the victim of sexually explicit, nonconsensual deepfake images using AI that were widely spread across social media platforms.[3] Perhaps more disturbingly, a trend has emerged in schools of students creating such images: "At schools across the country, people have used deepfake technology combined with real images of female students to create fraudulent images of nude bodies. The deepfake images can be produced using a cellphone."[4] As more of the population becomes aware of the potential to realistically fake images, video, and text, some will use the skepticism that creates to challenge the authenticity of real content, a phenomena coined the "liar's dividend."[5]

Relevant here, AI and specifically generative AI can spread misinformation regarding elections with ease, both in California and across the world:

> Artificial intelligence is supercharging the threat of election disinformation worldwide, making it easy for anyone with a smartphone and a devious imagination to create fake – but convincing – content aimed at fooling voters.

---

[1] Siddarth Srinivasan, *Detecting AI fingerprints: A guide to watermarking and beyond* (January 4, 2024) Brookings Institution, https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/#:~:text=Google%20also%20recently%20announced%20SynthID,model%20to%20detect%20the%20watermark. All internet citations are current as of June 22, 2024.

[2] Lonnie Lee Hood, *Experts Say That Soon, Almost The Entire Internet Could Be Generated by AI* (March 4, 2022) The Byte, https://futurism.com/the-byte/ai-internet-generation.

[3] Brian Contreras, *Tougher AI Policies Could Protect Taylor Swift – And Everyone Else – From Deepfakes* (February 8, 2024) Scientific American, https://www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/.

[4] Hannah Fry, Laguna Beach High School investigates 'inappropriate' AI-generated images of students (April 2, 2024) Los Angeles Times, https://www.latimes.com/california/story/2024-04-02/laguna-beach-high-school-investigating-creation-of-ai-generated-images-of-students.

[5] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (July 14, 2018) 107 California Law Review 1753 (2019), https://ssrn.com/abstract=3213954.

> It marks a quantum leap from a few years ago, when creating phony photos, videos or audio clips required teams of people with time, technical skill and money. Now, using free and low-cost generative artificial intelligence services from companies like Google and OpenAI, anyone can create high-quality "deepfakes" with just a simple text prompt.
>
> A wave of AI deepfakes tied to elections in Europe and Asia has coursed through social media for months, serving as a warning for more than 50 countries heading to the polls this year.
>
> "You don't need to look far to see some people ... being clearly confused as to whether something is real or not," said Henry Ajder, a leading expert in generative AI based in Cambridge, England.
>
> The question is no longer whether AI deepfakes could affect elections, but how influential they will be, said Ajder, who runs a consulting firm called Latent Space Advisory.
>
> As the U.S. presidential race heats up, FBI Director Christopher Wray recently warned about the growing threat, saying generative AI makes it easy for "foreign adversaries to engage in malign influence."[6]

On that last note, in February of this year, voters in New Hampshire received robocalls that are purported to have used an AI voice resembling President Joe Biden advising them against voting in the presidential primary and saving their vote for the November general election.[7] The examples are endless:

> Former President Donald Trump, who is running in 2024, has shared AI-generated content with his followers on social media. A manipulated video of CNN host Anderson Cooper that Trump shared on his Truth Social platform on Friday, which distorted Cooper's reaction to the CNN town hall this past week with Trump, was created using an AI voice-cloning tool.
>
> A dystopian campaign ad released last month by the Republican National Committee offers another glimpse of this digitally manipulated future. The online ad, which came after President Joe Biden announced his reelection campaign, and starts with a strange, slightly warped image of

[6] Ali Swenson & Kelvin Chan, *Election disinformation takes a big leap with AI being used to deceive worldwide* (March 14, 2024) Associated Press, https://apnews.com/article/artificial-intelligence-elections-disinformation-chatgpt-bc283e7426402f0b4baa7df280a4c3fd.
[7] Em Steck & Andrew Kaczynski, *Fake Joe Biden robocall urges New Hampshire voters not to vote in Tuesday's Democratic primary* (January 22, 2024) CNN, https://www.cnn.com/2024/01/22/politics/fake-joe-biden-robocall/index.html.

> Biden and the text "What if the weakest president we've ever had was re-elected?"
>
> A series of AI-generated images follows: Taiwan under attack; boarded up storefronts in the United States as the economy crumbles; soldiers and armored military vehicles patrolling local streets as tattooed criminals and waves of immigrants create panic.
>
> "An AI-generated look into the country's possible future if Joe Biden is re-elected in 2024," reads the ad's description from the RNC.
>
> The RNC acknowledged its use of AI, but others, including nefarious political campaigns and foreign adversaries, will not, said Petko Stoyanov, global chief technology officer at Forcepoint, a cybersecurity company based in Austin, Texas. Stoyanov predicted that groups looking to meddle with U.S. democracy will employ AI and synthetic media as a way to erode trust.[8]

Legislatures across the country are pushing legislation that would address this looming threat.

2. Materially deceptive content in political advertisements

This bill takes aim at "materially deceptive content" in elections communications. "Materially deceptive content" means audio or visual media that is intentionally digitally created or modified, such that the content would falsely appear to a reasonable person to be an authentic record of the content depicted in the media, including deepfakes. The bill prohibits any person, committee, or entity from knowingly distributing such advertisements or elections communications with this deceptive content when it portrays the following:

- A candidate for any federal, state, or local elected office in California portrayed as doing or saying something that the candidate did not do or say if the content is reasonably likely to harm the reputation or electoral prospects of a candidate.
- An elected official portrayed as doing or saying something in connection with an election in California that the elected official did not do or say if the content is reasonably likely to harm the reputation or electoral prospects of a candidate or is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

[8] David Klepper & Ali Swenson, *AI-generated disinformation poses threat of misleading voters in 2024 election* (May 14, 2023) PBS News, https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election.

- An elections official portrayed as doing or saying something in connection with an election in California that the elections official did not do or say if the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.
- A voting machine, ballot, voting site, or other property or equipment related to an election in California portrayed in a materially false way if the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

The bill provides one exception from these prohibitions. It provides that a candidate may portray themself as doing or saying something that the candidate did not do or say, if the content includes a clear disclosure, as specified, that states "This [category of content] has been manipulated." Concerns have been raised that this could be read as providing explicit legal authority for candidates to possibly engage in deceptive advertising or elections communications. The author has agreed to an amendment that instead clarifies that such portrayals are not subject to the provisions of this bill.

Recent amendments require this to be done with malice to amount to a violation. These prohibitions only apply 120 days before an election in California and, for the latter two categories, applies through 60 days after the election. These timelines limit the scope to periods when the outcome of the election, or the confidence in the election itself, is most vulnerable to such content.

Anyone receiving such advertisements or elections communications, any candidate or committee participating in the election, and any elections official are all given standing to seek injunctive relief to prohibit further distribution, with such actions given precedence in the courts. Prevailing plaintiffs are also entitled to reasonable attorney's fees and costs. In addition, such parties shall also have standing to bring an action for damages and fees and costs against a party in violation. Plaintiffs in these actions are required to establish violations by clear and convincing evidence.

According to the author:

> Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections.
>
> Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and

> deepfakes used in political campaign ads including mailers, television, radio, and robocalls.

3. Constitutional implications

As the bill prohibits certain forms of speech, it implicates the protections of the First Amendment of the United States Constitution, applied to the states by the Fourteenth Amendment. The First Amendment provides that "Congress shall make no law . . . prohibiting the freedom of speech." As interpreted by the courts, the First Amendment prevents the government from enacting any law or adopting any policy that burdens freedom of speech. In addition, Article I, Section 2 of the California Constitution guarantees to every person the freedom to "speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right." Moreover, the First Amendment not only protects the right to speak, as a logical corollary it protects the "right to receive information and ideas."[9] California courts have been clear that political expression in the context of campaigns of any manner should be given wide latitude:

> Hyperbole, distortion, invective, and tirades are as much a part of American politics as kissing babies and distributing bumper stickers and pot holders. Political mischief has been part of the American political scene since, at least, 1800.
>
> In any election, public calumny of candidates is all too common. "Once an individual decides to enter the political wars, he subjects himself to this kind of treatment. . . . [D]eeply ingrained in our political history is a tradition of free-wheeling, irresponsible, bare knuckled, Pier 6, political brawls." To endure the animadversion, brickbats and skullduggery of a given campaign, a politician must be possessed with the skin of a rhinoceros. Harry Truman cautioned would-be solons with sage advice about the heat in the kitchen.
>
> Nevertheless, political campaigns are one of the most exhilarating phenomena of our democracy. They bring out the best and the worst in us. They allow candidates and their supporters to express the most noble and, lamentably, the most vile sentiments. They can be fractious and unruly, but what they yield is invaluable: an opportunity to criticize and comment upon government and the issues of the day.
>
> The candidate who finds himself or herself the victim of misconduct is not without a remedy. Those campaign tactics which go beyond the pale are sanctionable under FPPC laws.

[9] *Stanley v Georgia* (1969) 394 U.S. 557, 564. Internal citations omitted

> It is abhorrent that many political campaigns are mean-spirited affairs that shower the voters with invective instead of insight. The elimination from political campaigns of opprobrium, deception and exaggeration would shed more light on the substantive issues, resulting in a more informed electorate. It would encourage more able people to seek public office. But to ensure the preservation of a citizen's right of free expression, we must allow wide latitude.[10]

The United States Supreme Court has emphasized the extraordinary protection afforded to political speech:

> Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression in order "to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people." Although First Amendment protections are not confined to "the exposition of ideas," "there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs,… of course includ[ing] discussions of candidates…." This no more than reflects our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." In a republic where the people are sovereign, the ability of the citizenry to make informed choices among candidates for office is essential, for the identities of those who are elected will inevitably shape the course that we follow as a nation. As the Court observed in *Monitor Patriot Co. v. Roy*, 401 U.S. 265, 272 (1971), "it can hardly be doubted that the constitutional guarantee has its fullest and most urgent application precisely to the conduct of campaigns for political office."[11]

This protection does not end where the truth of the speech does. "Although false statements of fact, by themselves, have no constitutional value, constitutional protection is not withheld from all such statements."[12] For instance, in the seminal opinion in *New York Times Co. v. Sullivan* (1964) 376 U.S. 254, 279-80, the court found the Constitution requires a rule that "prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' -- that is, with knowledge that it was false or with reckless disregard of whether it was false or not. The Supreme Court has expounded on this principle, providing nuance based on the knowledge of the speaker:

---

[10] *Beilenson v. Superior Court* (1996) 44 Cal. App. 4th 944, 954-55. Internal citations omitted.
[11] *Buckley v. Valeo* (1976) 424 U.S. 1, 14-15. Internal citations omitted.
[12] *People v. Stanistreet* (2002) 29 Cal. 4th 497, 505.

> Truth may not be the subject of either civil or criminal sanctions where discussion of public affairs is concerned. And since ". . . erroneous statement is inevitable in free debate, and . . . it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need . . . to survive' . . . ," only those false statements made with the high degree of awareness of their probable falsity demanded by *New York Times* may be the subject of either civil or criminal sanctions. For speech concerning public affairs is more than self-expression; it is the essence of self-government. The First and Fourteenth Amendments embody our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."
>
> The use of calculated falsehood, however, would put a different cast on the constitutional question. Although honest utterance, even if inaccurate, may further the fruitful exercise of the right of free speech, it does not follow that the lie, knowingly and deliberately published about a public official, should enjoy a like immunity. At the time the First Amendment was adopted, as today, there were those unscrupulous enough and skillful enough to use the deliberate or reckless falsehood as an effective political tool to unseat the public servant or even topple an administration. That speech is used as a tool for political ends does not automatically bring it under the protective mantle of the Constitution. For the use of the known lie as a tool is at once at odds with the premises of democratic government and with the orderly manner in which economic, social, or political change is to be effected. Calculated falsehood falls into that class of utterances which "are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. . . ." Hence the knowingly false statement and the false statement made with reckless disregard of the truth, do not enjoy constitutional protection.[13]

This bill implicates both the right to speak about elections, as well as the right to receive information regarding them. "Laws that burden political speech are subject to strict scrutiny, which requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest."[14]
However, this bill's language narrowly tailors the prohibitions in the bill to that speech afforded the least constitutional protection. "Materially deceptive content" requires that

[13] *Garrison v. Louisiana* (1964) 379 U.S. 64, 74-75. Internal citations omitted.
[14] *Citizens United v. FEC* (2010) 558 U.S. 310, 340. Internal citations omitted. It should be noted that while not controversial for the principle cited herein, this opinion is widely criticized for further tilting political influence toward wealthy donors and corporations.

it was intentionally created or altered such that the content falsely appears to be authentic. The bill requires the person, committee, or entity to knowingly distribute such material with malice, which means the person, committee, or other entity distributed the content knowing the materially deceptive content was false or with a reckless disregard for the truth. This mirrors the test laid out in *New York Times v. Sullivan*. In addition, many of the relevant cases stress that the level of burden placed on a defendant to defend their political speech is a factor to consider. For instance, the following was stated in *New York Times v. Sullivan*:

> A rule compelling the critic of official conduct to guarantee the truth of all his factual assertions -- and to do so on pain of libel judgments virtually unlimited in amount -- leads to a comparable "self-censorship." Allowance of the defense of truth, with the burden of proving it on the defendant, does not mean that only false speech will be deterred. Even courts accepting this defense as an adequate safeguard have recognized the difficulties of adducing legal proofs that the alleged libel was true in all its factual particulars.[15]

Responsive to this consideration, the bill requires a plaintiff bringing a claim pursuant to this bill, to prove the above factors by clear and convincing evidence.

Ultimately, this bill prohibits the knowing distribution of deceptive content with malice only at key points in the election cycle with an extremely compelling goal of safeguarding our democracy. Although, as with most restrictions on political speech, this bill may face legal challenge, it is arguably narrowly tailored to serve this compelling government interest to avoid improperly impinging on the constitutional guarantees of the First Amendment.

4. Stakeholder positions

A coalition of groups in support, including SEIU California and NextGen California, write:

> California is entering its first-ever generative artificial intelligence (AI) election, in which disinformation powered by generative AI will pollute our information ecosystems like never before. In a few clicks, using current technology, bad actors now have the power to create a false image of a candidate accepting a bribe, a fake video of an elections official "caught on tape" saying that voting machines are not secure, or a robocall of "Governor Newsom" incorrectly telling millions of Californians their voting site has changed. . . .

[15] *N.Y. Times Co. v. Sullivan*, at 279.

> AB 2839 seeks to solve these problems by preventing the use of deepfakes and disinformation -- targeting candidates, elected officials, and elections officials -- in political communications, and does so in a narrowly tailored way that is consistent with the First Amendment.

Writing in an oppose position, the Electronic Frontier Foundation argues the bill should be narrowed to focus on the direct publishers:

> We respectfully oppose your bill A.B. 2839, which not only bans the distribution of materially deceptive or altered content in relation to an election, but also places burdens on those unconnected to the creation of the content but who distribute it (internet websites, newspapers, etc.) regardless of whether they know of the prohibited manipulation. We recognize the complex issues raised by potentially harmful artificially generated election content. However, this bill's "exceptions" for only some types of republishers, and by requiring them to publish a disclaimer, does not reflect the full First Amendment protection due the republication of speech pertaining to matters of public interest by those not connected with the creation of the offending material.
>
> The First Amendment requires this distinction between those who create synthetic media and those not directly involved in it. The Fourth Circuit relied on this distinction in striking down a Maryland law that extended the reach of campaign finance law to include 'online platforms,' thus imposing disclosure requirements on them when they ran online ads. AB 2389, as written, suffers from the same constitutional defect.
>
> By extending beyond the direct publishers of the content and toward re-publishers, A.B. 2839 burdens and holding liable re-publishers of content in a manner that has been found unconstitutional.

SUPPORT

AFSCME California
Bay Rising
California Broadcasters Association
Catalyst California
Center for Countering Digital Hate
Chinese Progressive Association
City and County of San Francisco Board of Supervisors
Disability Rights California
Indivisible CA Statestrong
League of Women Voters of California
Move (mobilize, Organize, Vote, Empower) the Valley

NextGen California
Northern California Recycling Association
Partnership for the Advancement of New Americans
SEIU California
Youth Power Project

OPPOSITION

Directv Group, INC.
Dish Network, LLC
Electronic Frontier Foundation
Motion Picture Association
Streaming Innovation Alliance

RELATED LEGISLATION

Pending Legislation:

SB 942 (Becker, 2024) establishes the California AI Transparency Act, requiring covered providers to create and make freely available an AI detection tool to detect content as AI-generated and to include disclosures in content generated by the provider's system. SB 942 is currently in the Assembly Judiciary Committee.

SB 970 (Ashby, 2024) ensures that media manipulated or generated by artificial intelligence (AI) technology is incorporated into the right of publicity law and criminal false impersonation statutes. The bill requires those providing access to such technology to provide a warning to consumers about liability for misuse. SB 970 was held on suspense in the Senate Appropriations Committee.

AB 2355 (Wendy Carrillo, 2024) requires committees that create, publish, or distribute a political advertisement that contains any image, audio, or video that is generated or substantially altered using artificial intelligence to include a disclosure in the advertisement disclosing that the content has been so altered. AB 2355 is currently in this Committee.

AB 2655 (Berman, 2024) establishes the Defending Democracy from Deepfake Deception Act of 2024, which requires a large online platform to block the posting or sending of materially deceptive and digitally modified or created content related to elections, during specified periods before and after an election. It requires these platforms to label certain additional content inauthentic, fake, or false during specified periods before and after an election and to provide mechanisms to report content. AB 2655 is currently in this Committee.

AB 2930 (Bauer-Kahan, 2024) requires, among other things, a deployer and a developer of an automated decision tool to perform an impact assessment for any automated decision tool the deployer uses that includes, among other things, a statement of the purpose of the automated decision tool and its intended benefits, uses, and deployment contexts. AB 2930 requires a deployer to, at or before the time an automated decision tool is used to make a consequential decision, notify any natural person that is the subject of the consequential decision that an automated decision tool is being used to make, or be a substantial factor in making, the consequential decision and to provide that person with, among other things, a statement of the purpose of the automated decision tool. AB 2930 is currently in this Committee.

AB 3211 (Wicks, 2024) establishes the California Provenance, Authenticity and Watermarking Standards Act, which requires a generative AI system provider to take certain actions to assist in the disclosure of provenance data to mitigate harms caused by inauthentic content, including placing imperceptible and maximally indelible watermarks containing provenance data into content created by an AI system that the generative AI system provider makes available. AB 3211 also requires a large online platform, as defined, to, among other things, use labels to prominently disclose the provenance data found in watermarks or digital signatures in content distributed to users on its platforms, as specified. AB 3211 is currently in the Senate Appropriations Committee.

Prior Legislation: AB 730 (Berman, Ch. 493, Stats. 2019) prohibited the use of deepfakes depicting a candidate for office within 60 days of the election unless the deepfake is accompanied by a prominent notice that the content of the audio, video, or image has been manipulated. Additionally, AB 730 authorized a candidate who was falsely depicted in a deepfake to seek rapid injunctive relief against further publication and distribution of the deepfake.

PRIOR VOTES:

Senate Elections and Constitutional Amendments Committee (Ayes 6, Noes 0)
Assembly Floor (Ayes 59, Noes 4)
Assembly Appropriations Committee (Ayes 11, Noes 3)
Assembly Judiciary Committee (Ayes 8, Noes 2)
Assembly Elections Committee (Ayes 6, Noes 1)
****

EXHIBIT 6

Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 2839
Author: Pellerin (D) and Berman (D), et al.
Amended: 8/23/24 in Senate
Vote: 27 - Urgency

SENATE ELECTIONS & C.A. COMMITTEE: 6-0, 6/18/24
AYES: Blakespear, Allen, Menjivar, Newman, Portantino, Umberg
NO VOTE RECORDED: Nguyen

SENATE JUDICIARY COMMITTEE: 10-1, 7/2/24
AYES: Umberg, Wilk, Allen, Ashby, Caballero, Durazo, Laird, Roth, Stern, Wahab
NOES: Niello

SENATE APPROPRIATIONS COMMITTEE: 5-2, 8/15/24
AYES: Caballero, Ashby, Becker, Bradford, Wahab
NOES: Jones, Seyarto

ASSEMBLY FLOOR: 59-4, 5/22/24 - See last page for vote

SUBJECT: Elections: deceptive media in advertisements

SOURCE: California Initiative for Technology and Democracy

DIGEST: This bill prohibits the distribution of campaign advertisements and other election communications that contain media that has been digitally altered in a deceptive way. This bill also allows a court to issue injunctive relief prohibiting the distribution of such content, and to award general or special damages against the person that distributed the content.

Senate Floor Amendments of 8/23/24 specify that campaign advertisements and other election communications containing materially deceptive content that constitutes satire or parody are exempt from the provisions of the bill if there is an acknowledgement that the materially deceptive content does not represent any

actual event. The amendments also make additional clarifying changes, add urgency, and address chaptering issues with AB 2655 (Berman, 2024).

ANALYSIS:

Existing law:

1) Prohibits anyone from, until January 1, 2027, distributing within 60 days of an election materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

2) Prohibits anyone from, beginning January 1, 2027, producing, distributing, publishing, or broadcasting campaign material that contains a superimposed image of a candidate unless the campaign material includes a disclaimer that the picture is not an accurate representation of fact.

This bill:

1) Prohibits anyone, with malice, from knowingly distributing a campaign advertisement or other election communication containing materially deceptive content, during specified time periods, if:

   a) A candidate is portrayed as doing or saying something they did not do or say and the content is reasonably likely to harm the reputation or electoral prospects of the candidate;

   b) An elections official is portrayed as doing or saying something in connection with an election in California that the elections official did not do or say if the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests;

   c) An elected official is portrayed as doing or saying something in connection with an election in California that the elected official did not do or say if the content is reasonably likely to harm the reputation or electoral prospects of a candidate or is reasonably likely to falsely undermine confidence in the outcome of one or more election contests; or

   d) A voting machine, ballot, voting site, or other property or equipment related to an election in California is portrayed in a materially false way if the content is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

2) Provides the prohibition detailed above applies 120 days before any election in California and, with respect to content depicting an officer holding an election, conducting a canvass, or depicting elections equipment and materials, for 60 days after the election.

3) Permits a candidate, notwithstanding the prohibition detailed above, to portray themself as doing or saying something they did not do or say if the media includes a disclaimer stating "This (image/video/audio) has been manipulated."

4) Permits a recipient of materially deceptive content distributed in violation of this bill, a candidate or committee participating in the election, or an elections official, to seek:

   a) Injunctive or other equitable relief prohibiting the distribution of the media.

      i) Requires the court to award a prevailing plaintiff attorney's fees and costs, and provides such an action is entitled to precedence in court.

   b) General or special damages against the entity that distributed the materially deceptive content.

      i) Requires the court to award attorney's fees and costs to a prevailing party. Provides that this does not apply to a broadcast station or internet website that distributed the materially deceptive content if the broadcasting station or internet website did not create the content.

5) Provides that in any civil action brought under this bill, the plaintiff shall bear the burden of establishing the violation through clear and convincing evidence.

6) Provides this bill does not apply to:

   a) A broadcast station that broadcasts or a regularly-published news periodical that distributes any materially deceptive content prohibited by this bill if the media includes a clear acknowledgement it is not accurately representative;

   b) When an advertisement of other election communication containing materially deceptive content that constitutes as satire or parody if the communication includes a disclosure stating that the media has been manipulated; or

   c) A broadcast station when it is paid to broadcast materially deceptive content and either the following circumstances exist:

i) The broadcasting station can show it has prohibition and disclaimer requirements that are consistent with the requirements in this bill and that it has provided those requirements to each person or entity that purchased the advertisement.

ii) Federal law requires the broadcasting station to air advertisements from legally qualified candidates or prohibits the broadcasting station from censoring or altering the message.

7) Provides that specified provisions do not impose liability on an interactive computer service, as defined in Section 230(f)(2) of Title 47 of the United States Code.

8) Addresses chaptering issues with this bill and AB 2655.

9) Contains an urgency provision to take effect immediately.

Background

Manipulated Media in Campaign Communications. The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. The inaugural 1850 session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for."

California law today includes various provisions criminalizing deceptive tactics that undermine election integrity or interfere with voters' ability to participate in elections. This includes laws that prohibit distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur; prohibit the misleading use of government seals in campaign literature; and prohibit coercing or deceiving people into voting in a way that was inconsistent with the person's intent.

Artificial Intelligence and Elections. On June 4, 2024, the Senate Committee on Elections and Constitutional Amendments and the Assembly Committee on Elections held a joint information hearing focusing on AI and elections.

The purpose of the hearing was to inform and assist the Legislature in making informed decisions on legislation related to AI-generated and altered content. It became evident that the ease with which people can create and spread mis- and

disinformation creates a world where many people may have trouble determining what is fact and what is fiction. The development of increasingly advanced AI tools has made once time-consuming activities much easier to complete, while also enabling the completion of tasks that are otherwise too complex for humans to tackle alone.

State Action. In 2018, the Legislature approved and Governor Brown signed AB 3075 (Berman, Chapter 241, Statutes of 2018) to establish the Office of Elections Cybersecurity (OEC) in the Secretary of State's (SOS) office. The OEC has two primary missions. First, it is responsible for coordinating efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation.

In 2019, the Legislature approved and Governor Newsom signed AB 730 (Berman, Chapter 493, Statutes of 2019). AB 730 sought to address concerns that deepfake technology could be used to spread misinformation in political campaigns. Legislative analyses of AB 730 described "deepfake technology" as software capable of producing a realistic looking video of someone saying or doing something they did not actually say or do.

AB 730 prohibits anyone from distributing deceptive audio or visual media with actual malice and the intent to injure a candidate's reputation or to deceive a voter, unless the media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, it also applies to any intentional manipulation of audio or visual images where a reasonable person would be misled into believing it was authentic. Notably, AB 730 focused on materially deceptive representations of candidates, and not on deceptive media of other aspects of the electoral process. AB 730 included a January 1, 2023, sunset date, but in 2022 the Legislature approved AB 972 (Berman, Chapter 745, Statutes of 2022) to extend the sunset date to January 1, 2027.

Comments

1) *According to the Author:* "Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have

already started creating and distributing deepfake images, audio, and video content in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections.

"Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls."

2) *First Amendment Considerations.* The First Amendment to the United States (US) Constitution provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

This bill seeks to regulate the distribution of intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995, 514 US 334).

This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds would likely hinge on whether the court finds this bill's provisions to be narrowly tailored.

Related/Prior Legislation

AB 2355 (W. Carrillo, 2024) requires a campaign committee that creates, originally publishes, or originally distributes a political advertisement to include a

disclosure stating that the audio, image, or video was generated or substantially altered using AI.

AB 2655 (Berman, 2024) requires large online platforms with at least one million California users to develop and implement procedures to identify and remove materially deceptive content if certain conditions are met.

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

According to the Senate Appropriations Committee:

- This bill would not have a fiscal impact to the Secretary of State (SOS).
- By authorizing a claim by specified individuals and entities to enjoin distribution of a prohibited communication and seek damages, this bill may result in an increased number of civil actions that also receive precedence when filed in court. Consequently, the bill could result in potentially significant cost pressures to the courts; the magnitude is unknown (Trial Court Trust Fund (TCTF)). The specific number of new actions that could be filed under the bill also is unknown; however, it generally costs about $1,000 to operate a courtroom for one hour. Courts are not funded on the basis of workload, and increased pressure on TCTF may create a need for increased funding for courts from the General Fund. The enacted 2024-25 budget includes $37 million in ongoing support from the General Fund to continue to backfill TCTF for revenue declines.

SUPPORT: (Verified 8/27/24)

California Initiative for Technology and Democracy (source)
California Attorney General Rob Bonta
American Federation of State, County, and Municipal Employees, AFL-CIO
Asian Americans Advancing Justice – Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
Bay Rising
California Broadcasters Association
California Clean Money Campaign
Campaign Legal Center
Catalyst California
Center for Countering Digital Hate
Chinese Progressive Association
City and County of San Francisco Board of Supervisors

Courage California
Disability Rights California
Hmong Innovating Politics
Indivisible CA: Statestrong
Inland Empire United
League of Women Voters of California
MOVE (Mobilize, Organize, Vote, Empower) the Valley
NextGen CA
Northern California Recycling Association
Partnership for the Advancement of New Americans
SEIU California
TechEquity Action
Verified Voting
Voices for Progress Education Fund
Young People's Alliance
Youth Power Project

OPPOSITION: (Verified 8/27/24)

American Booksellers Association
Association of American Publishers
Authors Guild
Comic Book Legal Defense Fund
Entertainment Software Association
Electronic Frontier Foundation
First Amendment Coalition
Freedom to Read Foundation
Motion Picture Association
Streaming Innovation Alliance

ASSEMBLY FLOOR: 59-4, 5/22/24
AYES: Addis, Aguiar-Curry, Alanis, Alvarez, Arambula, Bains, Bennett, Berman, Boerner, Bonta, Bryan, Juan Carrillo, Wendy Carrillo, Connolly, Davies, Mike Fong, Gabriel, Garcia, Gipson, Grayson, Haney, Hart, Irwin, Jackson, Jones-Sawyer, Kalra, Lee, Low, Lowenthal, Maienschein, McCarty, McKinnor, Muratsuchi, Stephanie Nguyen, Ortega, Pacheco, Papan, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Rendon, Reyes, Rodriguez, Blanca Rubio, Santiago, Schiavo, Soria, Ting, Valencia, Villapudua, Waldron, Ward, Weber, Wicks, Wilson, Wood, Zbur, Robert Rivas
NOES: Vince Fong, Gallagher, Joe Patterson, Sanchez

NO VOTE RECORDED: Bauer-Kahan, Calderon, Cervantes, Chen, Megan Dahle, Dixon, Essayli, Flora, Friedman, Holden, Hoover, Lackey, Mathis, Jim Patterson, Luz Rivas, Ta, Wallis

Prepared by: Scott Matsumoto / E. & C.A. / (916) 651-4106
8/27/24 13:17:18

****** END ******

EXHIBIT 7

CONCURRENCE IN SENATE AMENDMENTS
AB 2839 (Pellerin and Berman)
As Amended August 23, 2024
2/3 vote. Urgency

SUMMARY

Prohibits the distribution of campaign advertisements and other election communications that contain media that has been digitally altered in a deceptive way, except as specified. Allows a court to issue injunctive relief prohibiting the distribution of such content, and to award general or special damages against a person that distributed the content, except as specified.

Senate Amendments

1) Broaden the bill to apply to content that is distributed through the internet.

2) Limit the bill's applicability to content related to elections in California.

3) Delete a provision of the bill that specified that it does not apply to content that is satire or parody, and instead provides that such content must contain a disclaimer, as specified, stating "This [image/audio/video] has been manipulated for purposes of satire or parody."

4) Specify that the bill does not apply to a broadcasting station that is paid to broadcast materially deceptive content if federal law requires the station to air the advertisement or if the station has its own prohibition and disclaimer requirements that are generally consistent with the requirements of this bill, as specified.

5) Specify that the bill does not impose liability on an interactive computer service, as defined under federal law.

6) Specify that an action for general or special damages under the bill may not be brought against a broadcasting station or internet website that distributed materially deceptive content but did not create the content.

7) Recast various provisions of the bill to improve clarity, and make other clarifying, technical, and conforming changes.

8) Add an urgency clause, allowing this bill to take effect immediately upon enactment.

9) Add double-jointing language to avoid chaptering problems with AB 2655 (Berman) of the current legislative session.

COMMENTS

The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. In 1850, the First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chapter 38, Statutes of 1850).

Advancements in technology have made it increasingly simple to produce false and misleading media that closely resembles authentic content. Moreover, platforms like social media have facilitated the rapid dissemination of deceptive media to large audiences at minimal cost. Given these developments, the potential threat posed by manipulated media to future elections' integrity may be more significant than in the past.

Past legislative efforts have addressed concerns about manipulated media's use to deceive voters during elections. Those laws, however, are limited, and are designed primarily to target the harms to *candidates* that may result from the distribution of manipulated media of those candidates. In contrast, this bill aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. Additionally, this bill targets media that portrays elections materials and equipment in materially deceptive ways. The author and supporters of this bill believe that these provisions will safeguard voters against deceitful media that could undermine trust in the electoral process.

A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the United States (US) and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds, then, likely would hinge on whether the court found this bill's provisions to be narrowly tailored.

This bill includes provisions to limit its scope to communications posing the greatest threat to election integrity in an effort to tailor its provisions. It applies only to communications that include media that was intentionally manipulated to be materially deceptive. Minor and cosmetic changes alone would not be considered to be materially deceptive. Furthermore, liability under this bill requires knowledge of the media's false portrayal of a candidate, elections official, elected official, or elections materials or equipment, or action with reckless disregard for the true portrayal of the candidate, official, or materials or equipment. Moreover, this bill applies only to communications that are reasonably likely to harm the reputation or electoral prospects of a candidate or to falsely undermine confidence in the outcome of one or more election contests.

Whether these limitations adequately protect this bill from a potential constitutional challenge is unclear. However, while these limitations may help protect the bill against a constitutional challenge, they may also make it harder for the bill to achieve its aims of limiting the spread of materially deceptive communications that have the potential to undermine election integrity.

The Senate amendments make several changes to narrow the bill's applicability to broadcast stations in response to opposition concerns, broaden the bill to apply to content that is distributed through the internet, and require materially deceptive content that is satire or parody to contain a disclaimer, among other changes.

Please see the policy committee analysis for a full discussion of this bill.

According to the Author
"Those trying to influence elections—conspiracy theorists, foreign states, online trolls, and even campaigns themselves—have already started creating and distributing deepfake images, audio, and video content, in the United States and around the world. This generative AI-fueled disinformation can affect voter behavior and undermine faith in our elections. Entering the 2024 election, millions of voters will not know what images, audio, or video they can trust, and their faith in election integrity and our democracy will be significantly diminished. AB 2839 will protect our democracy by limiting the spread of harmful disinformation and deepfakes used in political campaign ads including mailers, television, radio, and robocalls."

Arguments in Support
In support of this bill, the Campaign Legal Center writes, "AB 2839 is an important tool in the effort to address the role of AI in election advertising and disinformation. It would take several steps to prevent the use of deepfakes and disinformation in political communications, including communications targeting candidates, elected officials, and elections officials, and it provides a fast-track for injunctive relief to stop violations of the law. This approach is narrowly tailored and consistent with the First Amendment…While the risks of election manipulation, voter suppression, and misinformation all predate AI-based tools, AI provides bad actors with easy access to new tools to harm our democracy more easily and effectively. AI-fueled disinformation has the power to skew election results and undermine faith in our elections; states must act now to address this challenge head-on."

Arguments in Opposition
In opposition to this bill, the First Amendment Coalition writes, "[AB 2839] presents constitutional problems by authorizing an injunction against speech that is only 'reasonably likely' to harm reputation, as opposed to speech that has been found to be actually defamatory…By allowing courts to decide whether speech is 'reasonably likely' to harm 'electoral prospects' or 'undermine confidence' in elections, AB 2839 would improperly embroil courts in political disputes… In addition, AB 2839 radically expands the scope of liability by allowing any alleged 'recipient of materially deceptive content' to sue any person who distributes such content, regardless of whether the plaintiff was personally injured. AB 2839 threatens to flood the courts with complex litigation initiated by persons with no personal stake in the matter."

FISCAL COMMENTS

According to the Senate Appropriations Committee:

1) This bill would not have a fiscal impact to the Secretary of State.

2) By authorizing a claim by specified individuals and entities to enjoin distribution of a prohibited communication and seek damages, this bill may result in an increased number of civil actions that also receive precedence when filed in court. Consequently, the bill could result in potentially significant cost pressures to the courts; the magnitude is unknown (Trial Court Trust Fund (TCTF)). The specific number of new actions that could be filed under the bill also is unknown; however, it generally costs about $1,000 to operate a courtroom for one hour. Courts are not funded on the basis of workload, and increased pressure on TCTF may create a need for increased funding for courts from the General Fund. The enacted 2024-25 budget includes $37 million in ongoing support from the General Fund to continue to backfill TCTF for revenue declines.

VOTES:

ASM ELECTIONS: 6-1-1
YES: Pellerin, Bennett, Berman, Cervantes, Low, Weber
NO: Essayli
ABS, ABST OR NV: Lackey

ASM JUDICIARY: 8-2-2
YES: Kalra, Bryan, Connolly, Haney, Maienschein, McKinnor, Pacheco, Reyes
NO: Essayli, Sanchez
ABS, ABST OR NV: Dixon, Bauer-Kahan

ASM APPROPRIATIONS: 11-3-1
YES: Wicks, Arambula, Bryan, Calderon, Wendy Carrillo, Mike Fong, Grayson, Haney, Hart, Pellerin, Villapudua
NO: Sanchez, Jim Patterson, Ta
ABS, ABST OR NV: Dixon

ASSEMBLY FLOOR: 59-4-17
YES: Addis, Aguiar-Curry, Alanis, Alvarez, Arambula, Bains, Bennett, Berman, Boerner, Bonta, Bryan, Juan Carrillo, Wendy Carrillo, Connolly, Davies, Mike Fong, Gabriel, Garcia, Gipson, Grayson, Haney, Hart, Irwin, Jackson, Jones-Sawyer, Kalra, Lee, Low, Lowenthal, Maienschein, McCarty, McKinnor, Muratsuchi, Stephanie Nguyen, Ortega, Pacheco, Papan, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Rendon, Reyes, Rodriguez, Blanca Rubio, Santiago, Schiavo, Soria, Ting, Valencia, Villapudua, Waldron, Ward, Weber, Wicks, Wilson, Wood, Zbur, Robert Rivas
NO: Vince Fong, Gallagher, Joe Patterson, Sanchez
ABS, ABST OR NV: Bauer-Kahan, Calderon, Cervantes, Chen, Megan Dahle, Dixon, Essayli, Flora, Friedman, Holden, Hoover, Lackey, Mathis, Jim Patterson, Luz Rivas, Ta, Wallis

SENATE FLOOR: 32-6-2
YES: Allen, Archuleta, Ashby, Atkins, Becker, Blakespear, Bradford, Caballero, Cortese, Dodd, Durazo, Eggman, Glazer, Gonzalez, Hurtado, Laird, Limón, McGuire, Menjivar, Min, Newman, Padilla, Portantino, Roth, Rubio, Skinner, Smallwood-Cuevas, Stern, Umberg, Wahab, Wiener, Wilk
NO: Alvarado-Gil, Dahle, Grove, Jones, Niello, Seyarto
ABS, ABST OR NV: Nguyen, Ochoa Bogh

UPDATED

VERSION: August 23, 2024

CONSULTANT: Ethan Jones / ELECTIONS / (916) 319-2094 FN: 0004790

EXHIBIT 8

Date of Hearing: April 10, 2024

ASSEMBLY COMMITTEE ON ELECTIONS
Gail Pellerin, Chair
AB 2655 (Berman) – As Amended April 1, 2024

SUBJECT: Elections: deceptive audio or visual media.

SUMMARY: Requires large online platforms, as defined, to block the posting or sending of materially deceptive and digitally modified or created content related to elections, or to label that content, during specified periods before and after an election. Specifically, **this bill**:

1) Requires a large online platform (platform), using state-of-the-art, best available tools to detect digitally modified or created content, to develop procedures for blocking and preventing the posting or sending of materially deceptive and digitally modified or created content, and to block and prevent that content if the platform knows or should know that the content meets the following requirements, during a specified time period, of any of the following:

    a) A candidate portrayed as doing or saying something that the candidate did not do or say.

    b) An elections official portrayed as doing or saying something in connection with the performance of their elections-related duties that the official did not do or say.

    c) An elected official portrayed as doing or saying something that influences the election that the elected official did not do or say.

    d) A voting machine, ballot, voting site, or other property or equipment related to an election that is portrayed in a materially false way.

2) Prohibits a platform from preventing a candidate, notwithstanding the prohibition detailed above, from portraying themself as doing or saying something that the candidate did not do or say if the digital content includes a disclaimer stating: "This (image/video/audio) has been manipulated." Requires this disclaimer to comply with the following:

    a) In the case of visual media, requires the text of the disclaimer to appear in a size that is easily readable, as specified.

    b) In the case of a video, requires the disclaimer to appear for the duration of the video.

    c) In the case of media that consists of audio only, requires the disclaimer to be read in a manner that can be easily heard by the average listener at both the beginning and the end of the audio. For audio that is longer than two minutes, the disclaimer must also be included during the audio at intervals of not more than two minutes each.

3) Provides that the provisions detailed above apply only during the following time periods:

    a) Beginning 120 days before any election through the day of the election.

b) With respect to content pertaining to elections officials, or that depicts or pertains to elections equipment and materials, beginning 120 days before the election and ending on the 60th day after the election.

4) Requires a platform, using state-of-the-art, best available tools to detect digitally modified or created content, to develop procedures for labeling materially deceptive and digitally modified or created content that pertains to election processes and that is not subject to the blocking provisions outlined above, and to label such content as inauthentic, fake, or false if the platform knows or should know that the digitally modified or created content meets the requirements of this bill.

   a) Requires the label to permit users to click or tap on it and to inspect all available provenance data about the digitally modified or created content in an easy-to-understand format.

   b) Provides that the labeling requirement detailed above applies only during the following time periods:

      i) The period beginning one year before the election and through the day of the election that is specified in or implicated by the content.

      ii) The period beginning one year before the election process and through the final day of the election process that is specified in or implicated by the content.

      iii) If the content depicts or pertains to elections officials, the period beginning one year before the election or election process that is specified in or implicated by the content and ending on the 60th day after that election or the 60th day after the final day of that election process, as applicable.

5) Requires a platform to provide a way for Californians to report content that was not blocked or labeled as required. Requires the platform to respond within 36 hours and to describe any action taken.

6) Permits a Californian who reported content and who does not receive a response in 36 hours or who disagrees with the response, the Attorney General (AG), a district attorney, or a city attorney to seek injunctive or other equitable relief against a platform to compel compliance with this bill. Requires the court to award a prevailing plaintiff reasonable attorney's fees and costs. Provides that such an action is entitled to precedence in court, as specified.

7) Requires any label or disclaimer that must appear on content under this bill to appear in English, and in the same language as the content if the content isn't in English.

8) Requires a platform to maintain a copy of any content that it blocks or labels under this bill for at least five years from the election or election process specified or implicated in the content. Requires the platform to make that content available to the Secretary of State, the Fair Political Practices Commission, and researchers, if requested.

9) Provides that this bill does not apply to any of the following:

a) A regularly published online newspaper, magazine, or other periodical of general circulation that routinely carries news and commentary of general interest, and that publishes any materially deceptive and digitally altered or digitally created image, audio, or video recording that an online platform is required to block or label by this bill, if the publication contains a clear disclosure that the materially deceptive and digitally altered or digitally created image or audio or video recording does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.

b) Materially deceptive audio or visual media that constitutes satire or parody.

10) Defines the following terms, for the purposes of this bill:

a) "Election processes" to mean any government process related to an election, including, but not limited to, elections, candidates, vote counting, redistricting, and proceedings or processes of the electoral college.

b) "Materially deceptive and digitally modified or created content" to mean an image or an audio or video recording or other digital content, including a chatbot, that has been intentionally manipulated such that all of the following conditions are met:

i) The digital content is the product of digital manipulation, artificial intelligence (AI), or machine learning, including deep learning techniques, that merges, combines, replaces, or superimposes content onto an image or an audio or video recording, creating an image or an audio or video recording that appears authentic, or that otherwise generates an inauthentic image or an audio or video recording that appears authentic.

ii) The content contains a false portrayal of a candidate for elective office, an elected official, an elections official, or a voting machine, ballot, voting site, other property or equipment related to an election, or elections process. Provides that a "false portrayal" means the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if they were hearing or seeing the unaltered, original version of the content.

iii) The person or entity who attempted to post or send, or who did post or send, the content did so knowing the portrayal was false, or did so with reckless disregard for whether the portrayal was false. Provides that if the content is intentionally manipulated and contains a false portrayal, there is a rebuttable presumption that the person or entity knew the portrayal was false or that they acted with reckless disregard for whether the portrayal was false.

c) "Large online platform" to mean a public-facing internet website, web application, or digital application, including a social network, video sharing platform, advertising network, or search engine that had at least 1 million California users during the preceding 12 months.

11) Provides that content that contains only minor modifications that do not lead to significant changes to the perceived contents or meaning of the content are not "materially deceptive and digitally modified or created content" for the purposes of this bill, as specified.

12) Contains various findings and declarations and contains a severability clause.

EXISTING STATE LAW:

1) Prohibits a person, committee, or other entity, until January 1, 2027, from distributing with actual malice, within 60 days of an election at which a candidate for elective office will appear on the ballot, materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

   a) Defines "materially deceptive audio or visual media," for these purposes, as an image or an audio or visual recording of a candidate's appearance, speech or conduct that has been intentionally manipulated in a manner that both of the following are true about the image or audio or video recording:

      i) It would falsely appear to a reasonable person to be authentic; and,

      ii) It would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than the person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.

   b) Provides that this prohibition does not apply if the audio or visual media includes a disclaimer stating "This (image/video/audio) has been manipulated," and the disclaimer complies with specified requirements.

   c) Permits a candidate whose voice or likeness appears in deceptive audio or visual media distributed in violation of this provision to seek the following relief:

      i) Injunctive or other equitable relief prohibiting the distribution of the materially deceptive audio or visual media in violation of this bill. Provides that such an action is entitled to precedence in court, as specified.

      ii) General or special damages against the person, committee, or other entity that distributed that audio or visual media. Permits the court to award reasonable attorney's fees and costs to a prevailing party in such an action.

   d) Provides that in any civil action brought pursuant to these provisions, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

   e) Provides that this prohibition shall not be construed to alter or negate any rights, obligations, or immunities of an interactive service provider under Section 230 of the federal Communications Decency Act.

   f) Provides that this prohibition does not apply to any of the following:

i) A radio or television broadcasting station, as specified, in either of the following circumstances:

(1) When it broadcasts materially deceptive audio or visual media as part of a bona fide newscast, news interview, news documentary, or on-the-spot coverage of bona fide news events, if the broadcast clearly acknowledges through content or disclosure that there are questions about the authenticity of the audio or visual media, as specified.

(2) When it is paid to broadcast materially deceptive audio or visual media.

ii) An internet website, or a regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication, that routinely carries news and commentary of general interest, and that publishes materially deceptive audio or visual media covered by this prohibition, if the publication clearly states that the media does not accurately represent the speech or conduct of the candidate.

iii) Materially deceptive audio or visual media that constitute satire or parody. (Elections Code §20010, as amended by Section 3 of Chapter 745 of the Statutes of 2022)

2) Prohibits a person, firm, association, corporation, campaign committee, or organization, beginning January 1, 2027, with actual malice, from producing, distributing, publishing, or broadcasting campaign material, as defined, that contains either of the following types of pictures or photographs, as specified, unless the campaign material includes a disclaimer that the picture is not an accurate representation of fact:

a) A picture or photograph of a person or persons into which the image of a candidate for public office is superimposed.

b) A picture or photograph of a candidate for public office into which the image of another person or persons is superimposed. (Elections Code §20010, as amended by Section 4 of Chapter 745 of the Statutes of 2022)

EXISTING FEDERAL LAW provides, pursuant to Section 230 of the federal Communications Decency Act, that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. §230)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the Bill**: According to the author:

> AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential

to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in AI make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy.

2) **Threats of Manipulated Media in Campaign Communications**: The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. In 1850, the First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chapter 38, Statutes of 1850). California law today includes various provisions criminalizing deceptive tactics that undermine election integrity or interfere with voters' ability to participate in elections. This includes laws that prohibit distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur (Elections Code §18302); prohibit the misleading use of government seals in campaign literature (Elections Code §18304); and prohibit coercing or deceiving people into voting in a way that was inconsistent with the person's intent (Elections Code §§18573, 18573.5).

   Advancements in technology have made it increasingly simple to produce false and misleading media that closely resembles authentic content. Moreover, platforms like social media have facilitated the rapid dissemination of deceptive media to large audiences at minimal cost. Given these developments, the potential threat posed by manipulated media to future elections' integrity may be more significant than in the past.

   As described in greater detail below, past legislative efforts have addressed concerns about manipulated media's use to deceive voters during elections. Those laws, however, are limited, and are designed primarily to target the harms to *candidates* that may result from the distribution of manipulated media of those candidates. In contrast, this bill aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. Additionally, this bill targets media that portrays elections materials and equipment in materially deceptive ways. The author and supporters of this bill believe that these provisions will safeguard voters against deceitful media that could undermine trust in the electoral process.

3) **Recent Examples of Materially Deceptive Campaign Communications**: As evidence of the need for this bill, the author points to the following incidents, as reported in the media:

   - AI tools were used to create deepfake video ads of British Prime Minister Sunak on Facebook.

   - A Chinese disinformation campaign in Taiwanese elections made use of deepfakes, and AI-generated videos, images and audio clips.

   - AI tools additionally were used to disrupt elections in Argentina, Bangladesh, Pakistan, Slovakia.

- Governor Ron DeSantis created a deepfake of former President Trump hugging Anthony Fauci.

- AI was used by a democratic operative and a magician to generate deepfake audio of President Biden's voice that was used in a robocalls to dissuade voters from voting in the primary election.

4) **Previous Legislation Related to Materially Deceptive Media in Campaigns**: In 2019, in response to concerns that deepfake technology could be used to spread misinformation in political campaigns, the Legislature approved and Governor Newsom signed AB 730 (Berman), Chapter 493, Statutes of 2019. Deepfake technology refers to software capable of producing a realistic looking video of someone saying or doing something that they did not, in fact, say or do. This technology has advanced rapidly in recent years thanks to the use of AI to help train the software.

   AB 730 prohibits the distribution of materially deceptive audio or visual media with actual malice with the intent to injure a candidate's reputation or to deceive a voter into voting for or against a candidate, unless the materially deceptive audio or visual media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, but rather applies to any intentional manipulation of audio or visual images that results in a version that a reasonable observer would believe to be authentic. Nonetheless, the increasing availability and advancing capability of deepfake technology was the immediate impetus for that bill.

   AB 730 was designed as an update to California's "Truth in Political Advertising Act," a law enacted in 1998 (through the passage of AB 1233 (Leach), Chapter 718, Statutes of 1998) that prohibited campaign material that contains a picture of a person into which a candidate's image is superimposed, or contains a picture of a candidate into which another person's image is superimposed, except if a specified disclaimer was included. The Truth in Political Advertising Act was introduced in response to the use of photoshopped pictures in campaign materials, and accordingly was designed to target the manipulation of photographs in campaign materials. In the 20 years following its passage, however, it was never amended to update the law to address more modern techniques of manipulating campaign materials in a manner that can mislead voters. AB 730 replaced the Truth in Political Advertising Act with a law that regulates not only altered photographs in campaign materials, but also audio and video media that have been altered in a materially deceptive manner.

   AB 730 included a January 1, 2023 sunset date. In 2022, however, the Legislature approved AB 972 (Berman), Chapter 745, Statutes of 2022, which extended the sunset date to January 1, 2027. AB 972 did not otherwise change the provisions of AB 730. If the current January 1, 2027 sunset date is not repealed or extended, the original Truth in Political Advertising Act as enacted by AB 1233 of 1998 would go back into effect.

   Because the impetus for AB 730 was concern about the potential that people might create deepfake media appearing to be accurate representations of the conduct of candidates for office, its provisions apply exclusively to images or audio or video recordings of a candidate's appearance, speech, or conduct. Relatedly, candidates for elective office who are the target of materially deceptive media are the only entities that can seek injunctive relief or damages under AB 730. Materially deceptive images, audio, or video that appear in

campaign communications are not covered by AB 730 if that media is not of a candidate. For instance, if a candidate digitally manipulated video or a photo of a campaign rally to make the crowd look significantly larger than it actually was, such manipulation would not be covered by AB 730 as long as the manipulated image or video was not materially deceptive about a candidate's appearance, speech, or conduct. Similarly, manipulated and materially deceptive content in advertisements related to ballot measures, or in communications that seek to undermine confidence in the electoral process but that do not mention candidates directly, generally would not be covered by AB 730.

5) **Online Platforms and Materially Deceptive Content**: This is one of two bills being considered by the committee today that seek to address materially deceptive and digitally altered elections-related content in an effort to protect the integrity of elections in California. While the related bill that is being considered today (AB 2839 (Pellerin)) applies broadly to the distribution of such content through various mediums, this bill specifically targets the distribution of deceptive content through online platforms, including social media. Recognizing that those online platforms can facilitate the rapid spread of deceptive content, this bill seeks to minimize that potential by obligating large online platforms to block or label offending content. In order to do that, the platforms necessarily will need to be able to identify the content that must be blocked or labeled.

   In recognition that the regulation of the distribution of content can create free speech concerns, this bill contains various provisions that tailor the content to which it applies, such that it targets content that has the highest likelihood of deceiving voters and undermining electoral integrity. While that tailoring does limit the content that online platforms would be required to block or label, it also adds additional factors that platforms must consider in order to identify content that is required to be blocked or labeled under this bill.

   Along with other limitations, this bill applies only to content that (1) is distributed during specified time periods around elections and election processes, (2) includes media relating to elections or the electoral process in specified ways, (3) that was intentionally manipulated digitally to be materially deceptive, and (4) that is not satire or parody. Each of these limitations adds additional factors that online platforms would need to consider when determining whether a specific communication must be blocked or labeled by this bill.

   For example, in order to determine whether it must block content that *portrays a candidate for election as doing or saying something that the candidate did not do or say*, the platform would need to know not only that the person portrayed in the content was a candidate for office, but also the date (or dates) of the election when the candidate will appear on the ballot. Similarly, it would need to determine whether the candidate had actually said or done the thing that the candidate is portrayed as doing. While some of that information will be widely available and well known in some cases (e.g., the identity of major party candidates for President of the United States in presidential general elections and the dates of federal elections), it will be more arcane in other situations. Given the number of elections (including standalone local and special elections) and candidates (including write-in candidates and candidates for local elections in smaller jurisdictions) in California at any given time, making the determinations at scale about which content must be blocked or labeled likely will be considerably more challenging than making those determinations on a case-by-case basis in a court of law.

This bill includes numerous provisions that recognize that platforms will face challenges in making some of these determinations, and in limiting those platforms' obligations and liabilities accordingly. For instance, recent amendments to this bill provide for the large online platforms to use "state-of-the-art, best available tools" for detecting digitally modified or created content, recognizing that the identification of such content with perfect accuracy is impossible. Other recent amendments provide that an online platform is obligated to block or label content only if the platform "knows or should know" that the content meets the requirements of the bill, and provide that the bill's requirements relating to content portraying an elections official applies only if the platform knows or should know that the person is an elections official. Furthermore, unlike the related legislation that targets materially deceptive election content more broadly, this bill does not provide for damages to be awarded against platforms that fail to comply with their obligations. Instead, the only legal relief available under this bill is injunctive relief, and a person (other than the AG, a district attorney, or a city attorney) would be required to report the content to the platform and give the platform an opportunity to block or label the content before the person could seek that relief. Notwithstanding these provisions, the extent to which large online platforms will be able to accurately block and label materially deceptive elections-related content at scale, as contemplated by this bill, is unclear.

6) **Free Speech Considerations**: The First Amendment to the United States (US) Constitution, which also applies to states under the Fourteenth Amendment, provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

   This bill seeks to regulate the distribution by online platforms of media containing intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

   This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds, then, likely would hinge on whether the court found this bill's provisions to be narrowly tailored.

   As discussed in more detail above, this bill includes provisions to limit its scope to communications posing the greatest threat to election integrity. Whether these limitations adequately protect this bill from a potential constitutional challenge is a question that falls more squarely within the jurisdiction of the Assembly Judiciary Committee, where this bill will be heard next if it is approved by this committee. However, while these limitations may help protect the bill against a constitutional challenge, they may also make it harder for the

bill to achieve its aims of limiting the spread of materially deceptive communications that have the potential to undermine election integrity.

7) **Arguments in Support**: The sponsor of this bill, the California Initiative for Technology & Democracy, a Project of California Common Cause, writes in support:

> Those trying to influence campaigns – conspiracy theorists, foreign states, online trolls, and candidates themselves – are already creating and distributing election-threatening deepfake images, audio, and video content in the US and around the world. This threat is not imaginary: generative AI has been used in various ways – most of them deeply deceptive – to influence the national elections in Slovakia, Bangladesh, Argentina, Pakistan, and elsewhere, including in our own country. Examples of this occurring in U.S. elections include Ron Desantis using AI-generated images to attack his opponent in his presidential run, foreign states caught attempting to influence American politics through social media, and just this month, a supporter of former President Trump creating a deepfake image of Trump with Black Americans designed to persuade Black voters to support Trump…
>
> [AB] 2655 strikes the right balance by seeking to ban, for a strictly limited time before and after elections, the online spread of the worst deepfakes and disinformation maliciously intended to prevent voters from voting or getting them to vote erroneously based on fraudulent content. The bill also requires that other fake online content related to elections and elections processes (such as redistricting), which is also designed to undermine election procedures and democratic institutions, must be labeled as fake, again just for a limited time. The bill only applies to the largest online platforms with the greatest reach of potential election disinformation, and we believe it is fully implementable today based on tools these companies already possess. The companies covered by the bill's requirements are all already subject to similar requirements under the European Union's Digital Services Act, which is designed to, among other things, crack down on election interference.
>
> AB 2655's approach is narrowly tailored and does not extend the law to hot button controversies or inflammatory claims – it does not ask social media platforms to adjudicate controversial opinions post by post. It simply stops the use of obviously, demonstrably untrue and provably false content meant to impermissibly influence our elections at peak election times.

8) **Arguments in Opposition**: A joint letter of opposition submitted by Chamber of Progress, Computer and Communications Industry Association, NetChoice, Software & Information Industry Association, and TechNet states:

> Responsible digital services providers take aggressive steps to moderate dangerous and illegal content, consistent with their terms of service. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review. In 2021, a number of online businesses announced that they had been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices to

ensure a safer and more trustworthy internet, and have recently reported on the efforts to implement these commitments.

AB 2655 appears to be based on the false assumption that online platforms definitively know whether any particular piece of content has been manipulated in such a way that is defined under the bill. While digital services may employ tools to identify and detect these materials with some degree of certainty, it is an evolving and imperfect science in its current form. AB 2655 also presumes that online platforms are an appropriate arbiter of deciding what constitutes accurate election information. However, most digital services are not equipped with the tools or expertise to make such judgments.

AB 2655 would impose significant operationally and practically challenging requirements on large online platforms who may not be best suited to achieve the bill's laudable and important goal of ensuring California's elections remain free and fair.

9) **Related Legislation**: AB 2355 (Wendy Carrillo), which is also being heard in this committee today, requires a political advertisement that is generated in whole or in part using AI to include a disclaimer stating that fact.

AB 2839 (Pellerin), which is also being heard in this committee today, prohibits the distribution of campaign advertisements and other election communications that are materially deceptive and digitally altered or created, except as specified.

10) **Double-Referral**: This bill has been double-referred to the Assembly Judiciary Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

California Initiative for Technology & Democracy, a Project of California Common Cause (Sponsor)
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
California Clean Money Campaign
California State Sheriffs' Association
California Voter Foundation
Courage California
Disability Rights California
Indivisible CA Statestrong
Inland Empire United
The Partnership for the Advancement of New Americans
Verified Voting

Opposition

Chamber of Progress
Computer and Communications Industry Association

Electronic Frontier Foundation
NetChoice
Oakland Privacy (unless amended)
Software & Information Industry Association
TechNet

Analysis Prepared by: Ethan Jones / ELECTIONS / (916) 319-2094

EXHIBIT 9

Date of Hearing: April 23, 2024

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
AB 2655 (Berman) – As Amended April 1, 2024

As Proposed to be Amended

SUBJECT: DEFENDING DEMOCRACY FROM DEEPFAKE DECEPTION ACT OF 2024

KEY ISSUE: SHOULD LARGE ONLINE PLATFORMS BE REQUIRED TO BLOCK (OR IN SOME CASES LABEL) MATERIALLY DECEPTIVE AND DIGITALLY MODIFIED OR CREATED CONTENT RELATED TO AN ELECTION OR ELECTION PROCESS, DURING A PRESCRIBED PERIOD OF TIME BEFORE OR AFTER AN ELECTION?

SYNOPSIS

According to the author, disinformation powered by Artificial Intelligence (AI), which can be distributed to millions of social media users in an instant, poses a serious threat to our political discourse, our elections, and indeed our democracy. For example, "deepfakes" can generate false sounds and images that could lead to the most discerning viewer to falsely conclude that a candidate, elected official, or election worker said or did something they did not do. Such disinformation not only distorts the truth, it has the potential to undermine people's confidence in our political institutions. While disinformation can threaten political discourse at any time, the author believes that it is especially harmful during an election season, when uncorrected disinformation may influence an election result or create false concerns about the legitimacy of an election in its immediate aftermath.

This bill, therefore, would require a large online platform to block "materially deceptive and digitally modified or created" content that portrays any candidate, elected official, or elections official doing or saying something they did not do or say; it would also require them to block deceptive material that concerns voting machines, ballots, voting sites, or other procedures or equipment related to an election. In addition, deceptive material about broader "elections processes," that are not subject to blocking requirement, would need to contain a label that they are materially deceptive and digitally modified. The bill would allow any resident of California to inform the platform that covered material had not been properly blocked or labeled, and if the platform does not respond within 36 hours, or if the reporting resident does not agree with the response, the resident may bring an action for injunctive relief. The bill would also allow the Attorney General, or any district attorney or city attorney, to also seek injunctive relief.

This bill passed out of the Assembly Elections Committee on a 6-1 vote. It is sponsored by the California Initiative for Technology and Democracy, a project of California Common Cause, and supported by several political reform groups and labor organizations, among others. The bill is opposed by groups representing the information and technology industry and by ACLU Action California. The opposition argues that the bill would be ineffective, unconstitutional, and preempted by federal law. The author will take several definitional amendments in this Committee, which are reflected in the Summary, below, and discussed in the analysis.

SUMMARY: Requires large online platforms, as defined, to block the posting or sending of materially deceptive and digitally modified or created content related to elections, or to label that content, during specified periods before and after an election. Specifically, **this bill**:

1) Makes findings and declarations about the growing use of generative artificial intelligence (AI), deepfakes, and related technologies to disseminate disinformation that distorts our electoral process and undermines trust in elections.

2) Requires a large online platform (platform), using state-of-the-art, best available tools to detect digitally modified or created content, to develop procedures for blocking and preventing the posting or sending of materially deceptive and digitally modified or created content, and to block and prevent that content if the platform knows or should know that the content meets the following requirements, during a specified time period, of any of the following:

   a) A candidate portrayed as doing or saying something that the candidate did not do or say.

   b) An elections official portrayed as doing or saying something in connection with the performance of their elections-related duties that the official did not do or say.

   c) An elected official portrayed as doing or saying something that influences the election that the elected official did not do or say.

   d) A voting machine, ballot, voting site, or other property or equipment related to an election that is portrayed in a materially false way.

3) Prohibits a platform, notwithstanding the above, from preventing candidates from posting deceptive and manipulated material *about themselves* so long as the content includes a prescribed disclaimer.

4) Provides that the above prohibitions apply only during the period 120 days before and through election day; however, they apply to content relating to elections officials, voting sites, voting machines, ballots, or related equipment from 120 days before the election to 60 days after the election.

5) Requires a platform to develop procedures for labeling materially deceptive and digitally modified or created content that pertains to election processes, but that is not subject to the blocking provisions above. Requires the label to indicate that the content is inauthentic, fake, or false if the platform knows or should know as much. Provides that the labeling requirement applies during the period beginning one year before the election or election process, as specified.

6) Requires the platform to provide a way for Californians to report content that was not blocked or labeled as required, and requires the platform to respond to the report within 36 hours and to describe any actions taken. If the platform does not respond within 36 hours, or if the reporting resident disagrees with the response, the reporting resident may bring an action for injunctive or other equitable relief, and a prevailing plaintiff may recover reasonable attorney's fees and costs. Allows the Attorney General, a district attorney, or a city attorney to similarly seek injunctive relief and obtain fees and costs.

7) Specifies that the provisions of this bill do not apply to a regularly published online newspaper, magazine, or periodical, as specified.

8) Defines the following terms for purposes of the above as follows:

   a) "Elections official" means any of the following: an elections official as defined in Elections Code Section 320; the Secretary of State and their staff; a temporary worker, poll worker, or member of a precinct board; any other person charged with holding or conducting an election, a canvas, or performing another election-related duty.

   b) "Election processes" means any government process related to an election, including, but not limited to, elections, candidates, vote counting, redistricting, and proceedings or processes of the Electoral College.

   c) "Materially deceptive and digitally modified or created content" means an image or an audio or video recording or other digital content, including a chatbot, that has been intentionally manipulated such that all of the following conditions are met:

      i) The digital content is the product of digital manipulation, artificial intelligence, or machine learning, including deep learning techniques, that merges, combines, replaces, or superimposes content onto an image or an audio or video recording, creating an image or an audio or video recording that appears authentic, or that otherwise generates an inauthentic image or an audio or video recording that appears authentic, and that contains a false portrayal of any of the following: a candidate for elective office, elected official, elections official, voting machine, ballot, voting site, other property or equipment related to an election, or elections process; and provides that "false portrayal" means the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if they were hearing or seeing the unaltered, original version of the content.

      ii) The person or entity who attempted to post or send, or who did post or send, the content did so knowing the portrayal was false, or did so with reckless disregard for whether the portrayal was false. If the content is intentionally manipulated and contains a false portrayal as specified in subparagraph (A), there shall be a rebuttable presumption that the person or entity knew the portrayal was false or that they acted with reckless disregard for whether the portrayal was false.

   d) Clarifies that "Materially deceptive and digitally modified or created content" does not include any image or audio or video recording that contains only minor modifications that do not lead to significant changes to the perceived contents or meaning of the content. Minor changes include changes to the brightness or contrast of images, removal of background noise in audio, and other minor changes that do not impact the content of the image or audio or video recording.

   e) "Large online platform" means a public-facing internet website, web application, or digital application, including a social network, video sharing platform, advertising network, or search engine that had at least 1 million California users during the preceding 12 months.

f) "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

EXISTING LAW:

1) Prohibits a person, committee, or other entity, until January 1, 2027, from distributing with actual malice, within 60 days of an election at which a candidate for elective office will appear on the ballot, materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

   a) Defines "materially deceptive audio or visual media," for these purposes, as an image or an audio or visual recording of a candidate's appearance, speech or conduct that has been intentionally manipulated in a manner that both of the following are true about the image or audio or video recording: (1) It would falsely appear to a reasonable person to be authentic; and (2) it would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than the person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.

   b) Provides that this prohibition does not apply if the audio or visual media includes a disclaimer stating "This (image/video/audio) has been manipulated," and the disclaimer complies with specified requirements.

   c) Permits a candidate whose voice or likeness appears in deceptive audio or visual media distributed in violation of this provision to seek injunctive relief, as specified, and general or special damages and reasonable attorney's fees and costs, as specified. Specifies that in any civil action brought pursuant to these provisions, the plaintiff bears the burden of establishing the violation through clear and convincing evidence.

   d) Provides that this prohibition shall not be construed to alter or negate any rights, obligations, or immunities of an interactive service provider under Section 230 of the federal Communications Decency Act.

   e) Provides that this prohibition does not apply to a radio or television broadcasting station; an internet website; a regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication; or media that constitute satire or parody. (Elections Code Section 20010.)

2) Prohibits a person, firm, association, corporation, campaign committee, or organization, beginning January 1, 2027, with actual malice, from producing, distributing, publishing, or broadcasting campaign material, as defined, that contains either of the following types of pictures or photographs, as specified, unless the campaign material includes a disclaimer that the picture is not an accurate representation of fact:

   a) A picture or photograph of a person or persons into which the image of a candidate for public office is superimposed.

b) A picture or photograph of a candidate for public office into which the image of another person or persons is superimposed. (Elections Code Section 20010.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: According to the author:

> AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in AI make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy.
>
> Therefore, in order to ensure California elections are free and fair, online platforms must prevent the online spread of election-related deceptive deepfakes and disinformation meant to prevent voters from voting or to deceive them based on fraudulent content.

Existing laws maintaining "election integrity." As aptly noted in the analysis of this bill by the Assembly Elections Committee, the "use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon," nor are the laws "aimed at curbing such practices" new. Indeed, in 1850, the First Session of the California State Legislature created penalties for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for." (Chapter 38, Statutes of 1850.) Existing California law has greatly elaborated on these initial legislative efforts. For example, provisions in the Elections Code prohibit the distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur; prohibit the misleading use of government seals in campaign literature (Elections Code Section 18304); and prohibit coercing or deceiving people into voting in a way that is inconsistent with the person's intent (Elections Code Sections 18302, 18304, 18573 and 18573.5).

In the last five years, the Legislature has turned its attention to "materially deceptive" audio and visual materials that portray a candidate. For example, AB 730 (Chap. 493, Stats. 2019) responded to reports that so-called "deepfake" technology, a software that allows someone to produce audios and videos that look and appear remarkably real to even the most discerning person. For example, in 2018, BuzzFeed and the film director Jordan Peele published a very realistic-looking deepfake showing former President Obama calling then-President Donald Trump a "total and complete dipshit." Obama did not say that. Peele and BuzzFeed did not use the video to try to influence a political election – indeed halfway through the video the ruse was revealed – but to show the potential for abuse of deepfake technology. Responding to this and similar reports, AB 730 prohibited the distribution of materially deceptive audio or visual media with the intent to injure the candidate's reputation or to deceive a voter into voting for or against a candidate.

AB 730 was itself an amendment to California's "Truth in Political Advertising Act" of 1998, which had prohibited campaign material that deceptively altered a picture of a candidate (for example by superimposing one person's image upon another) unless the picture contained a disclaimer. This 1998 bill was introduced in response to the use of technologies like "photo

shopping," which now seem quaint compared to deepfakes, including deepfakes generated by artificial intelligence. The bill now before the Committee, like AB 730 before it, is apparently an effort to stay one step ahead of evolving technologies, which not only create more realistic-looking deceptions, but make it possible to quickly create, alter, and distribute fake images to millions of people in the blink of an eye (or the click of a mouse).

This bill and existing law: who? AB 2655 elaborates upon and modifies existing law in a variety of ways. Most significant, existing law prohibits *a person, committee, or other entity* from distributing, with actual malice, "materially deceptive" audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate. Existing law prohibits the distribution of such material within 60 days of the election in which the targeted candidate is running for office. The prohibitions in AB 2655, on the other hand, do not apply to the person or entity that created the materially deceptive material, but to the "large online platform" on which it is posted. AB 2655 requires the online platform to develop and implement procedures to block or prevent the posting of the covered content.

This bill and existing law: what? This bill also differs from existing law in terms of covered content. Existing law applies only to manipulated material that misrepresents the "candidate" saying or doing something the candidate did not do or say. This bill similarly applies to content deceptively depicting the candidate, but also applies to images portraying an "elections official" doing or saying something they did not do or say, as well as images depicting a voting machine, ballot, voting site, or voting equipment in a materially false way. In addition, this bill would require the platform to label (but not necessarily block) materially deceptive content about "election processes" (as opposed to a specific candidate, election official, or voting site). Although the distinction between what material must be blocked versus what material must be labeled is not entirely clear, the intent of the author and sponsor is that the more the material singles out a particular candidate or election official, the more it must be blocked; whereas material that deals with "election processes" more generally need only be labeled. *The author has agreed to work with the Committee as the bill moves forward to clarify the distinction between the blocking and labeling requirements.*

This bill and existing law: when? AB 2655 also expands and modifies the relevant time period that prohibitions are in force. Existing law prohibits someone from distributing deceptive material during the 60-day period before an election. This bill, however, requires the platform to block covered material a period beginning 120 days before the election and through the day of the election. However, if the deceptive material pertains to an election official, or deceptively depicts a voting machine, ballot, voting site, or property or equipment related to an election, the platform must also block the content for 60 days *after* the election. Presumably, this post-election period is intended to prevent false claims – similar to those made in 2020 – that the election process was irregular or otherwise "rigged." The labeling requirement covers an even larger time frame; it applies during the period beginning *one year* before the "election." The bill also requires labeling for the period beginning one year before an "election process." "Election processes" – as opposed to an "election" – is defined to include any government process "related" to an election, "including, but not limited to," elections, candidates, vote counting, redistricting, and proceedings or processes of the electoral college." Because an "election" has a known date, it should be fairly easy for the platform to figure out when the year-long labeling period starts. However, if the platform must also label one year prior to an "election process," when does a process like "redistricting" start? Does it start with each new census? Does it start when the legislative body (or in some states a commission) meet to draw up new district lines?

Moreover, the definition of "election process" is not limited to the items listed, expressly stating "including, but is not limited to,' those items. *As discussed above, the author has agreed to work with the Committee as the bill moves forward to clarify the distinction between materials that the platform is required to "block" and those it is required to "label."*

This bill and existing law: how enforced? In addition to differences as to who, what, and when, this bill also differs in how violations would be enforced. Existing law permits only the "candidate" whose voice or likeness appears in the deceptive material to bring an action for injunctive relief, general or special damages, and reasonable attorney's fee and cost. However, under existing law the candidate bears the burden of establishing a violation by "clear and convincing evidence." Enforcement provisions in this bill are much different. The bill allows any "California resident" to report to the platform that content was not blocked or labeled as required. If the platform does not respond within 36 hours, *or if the resident disagrees with the response*, the resident may seek injunctive relief to compel compliance and, if the resident prevails, shall be awarded reasonable attorney's fees and costs. Thus, not only can any California resident – not just a person depicted or otherwise affected – seek injunctive relief, they apparently do not have the burden of proving a violation by clear and convincing evidence. If they "disagree" with the platform's response, that's enough; they can seek injunctive relief and a court would decide to issue on the likelihood of success on merits, the general rule for injunctive relief. *The author may wish to consider, as the bill moves forward, increasing the standard of proof to the higher clear and convincing evidence; and limiting who may seek relief.*

First Amendment concerns. Because this bill imposes a *government* mandate that online platforms must block expressive material based upon its content, it implicates the First Amendment. The First Amendment provides that "Congress shall make no law . . . prohibiting the freedom of speech." As interpreted by the courts and incorporated against the states by the due process clause of the 14th Amendment, the First Amendment prevents any government entity (not just Congress) from enacting any law or adopting any policy that burdens freedom of speech. In addition, Article I, Section 2 of the California Constitution guarantees to every person the freedom to "speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right." Moreover, the First Amendment not only protects the right to speak, as a logical corollary it protects the "right to receive information and ideas." (*Stanley v Georgia* (1969) 394 U.S. 557, 564.) This bill would interfere with both the expression and reception of information based upon its content. Moreover, not only does this bill single out particular content, the content relates to political candidates and elections. This is potentially problematic because the First Amendment affords the "broadest protection" to the "discussion of public issues" and "political expression in order to assure the unfettered interchange of ideas for the bringing about of political and social changes desired by the people." (*McIntyre v Ohio Election Commission* (1997) 514 U.S. 334.) It is difficult to imagine any content more related to "political expression" and "discussion of public issues" than content about candidates and elections. The fact that the bill restricts speech that is "materially deceptive" or "false" does not matter, for the U.S. Supreme Court has been unequivocal that the First Amendment protects even "false" speech. The remedy for false speech is more true speech, and false speech tends to call forth true speech. (*United States v Alvarez* (2012) 567 U.S. 709.)

The bill will likely meet the "compelling interest" threshold, if not the "narrowly tailored" threshold. The right to free speech is not absolute. As Justice Holmes noted in a dissenting opinion over a century ago, the First Amendment does not protect a right to falsely cry fire in a crowded theater. (*Schenck v. United States* (1919) 249 U.S. 47.) The proponents of this bill may,

not unreasonably, think that pervasive disinformation about candidates and elections, especially during an election season, is just as dangerous. In reviewing the law, the Court would apply strict scrutiny. This means that government can impose even content-based restrictions on protected speech *if* they have a "compelling government interest" *and* they use "narrowly tailored means" to achieve that interest.

Even the opponents of this bill appear to concede that maintaining "election integrity" is a "weighty" and, presumably, "compelling" government interest. Therefore, it seems likely that if this bill is enacted and subsequently challenged, a court will accept that there is a "compelling interest" but still need to consider whether the "means" are "narrowly tailored." The opponents of this measure claim that it is *not* narrowly tailored. They contend that while covered platforms may have state-of-the-art tools that allow them to identify content that has been "digitally modified," there is no technology to determine if content is "materially deceptive." The bill defines "materially deceptive," in relevant part, to mean content that is "intentionally manipulated" so that it appears "authentic" but contains a "false portrayal" of a candidate, elected official, elections official, voting machine, ballot, voting site, other property or equipment related to an election, or elections process. The purpose of narrow tailoring is to ensure that no more speech is infringed or burdened than is necessary. However, the opponents of this bill – both the industry groups and the ACLU – believe that with no sure means to determine what is "materially deceptive," the platforms will err on the side of blocking content, thus burdening more speech than is necessary.

The findings and declarations in the bill state that the "labeling information required by this bill is narrowly tailored to provide consumers with factual information about the inauthenticity of particular images, audio, video, or text content in order to prevent consumer deception." Tellingly, there is no similar claim about the blocking requirement being narrowly tailored. In any event, it will be a court – not the findings and declarations of the bill – that will determine whether the bill is narrowly tailored. The court may consider, for example, if there are other less restrictive and more effective means of protecting election integrity.

Section 230 concerns and "editorial discretion." In addition to implicating the First Amendment, this bill may also be preempted by Section 230 of the federal Communications Decency Act. In relevant part, Section 230 provides two express protections for online platforms and their ability to moderate online content. First, Section 230 declares that an online platform cannot be held liable for content posted by third parties. The rationale for this immunity is premised on the idea that online platforms, unlike newspapers, do not exercise editorial discretion; rather, like telephone companies or "common carriers" they are merely a conduit for the expression of ideas by others. Those others, not the platform, are liable for any harm caused by the content. Second, somewhat in tension with this immunity, Section 230 expressly provides that online platforms are not liable if they block or remove material because they disapprove of its content. While it is important to remember that the First Amendment is distinct from Section 230, this protection flows from First Amendment principles. First, because the online platform is not a government actor, it cannot violate the First Amendment. Second, as a private actor, the platform has its own First Amendment right not to be associated with speech it finds objectionable. Some scholars have noted that the two protections in Section 230 are based on contrary premises. Immunity from liability from postings by third parties assumes that platforms *do not* exercise editorial discretion. Their right to remove content without liability, and their own free speech claims, on the other hand, assume that they *do* exercise editorial discretion. [For a concise overview of Section 230 and its intersection with the First Amendment, see Bollinger

and Stone, *Social Media, Freedom of Speech, and the Future of our Democracy* (Oxford University Press, 2022), especially pp. xxiii-xl; on efforts to reform Section 230, see pp.103-120.] Whatever the merits or demerits of Section 230 may be, it is federal law and appears to grant social media platforms the right to moderate content on their platforms and immunizes them from liability for content posted by the third party.

Cases pending before the U.S. Supreme Court. In February of this year, the U.S. Supreme Court heard arguments about two state laws that may have far-reaching consequences for both First Amendment case law and the status of Section 230. Largely in response to social media platforms barring former President Donald Trump from their platforms in the wake of the January 6 riots, both Texas and Florida enacted laws that limited the ability of social media platforms to control content on their platforms. The Florida law fines platforms if they ban a candidate for office in their state, and requires platforms to disclose information about their moderation policies. The Texas law prohibits platforms from removing content based on its "viewpoint." Both of these laws directly challenge the provision in Section 230 that expressly allows platforms to remove content. Both laws also raise First Amendment concerns about the platforms' right not to be associated with views with which they disagree. Both laws provide an interesting point of comparison with the bill under review: Texas and Florida *prohibit* a platform from denying access to certain people or blocking content on certain topics, while this bill would *require* the platforms to remove content. The Court is expected to issue a ruling in June of this year. How that ruling would affect this bill is unclear, especially given that this bill moves in the opposite direction of the Florida and Texas laws. However, if the Court decides in favor of the platforms – which many commentators think they will, at least in part – it might suggest that the Court believes that platforms should be given more freedom to self-moderate content without state interference. (*See* David McCabe, "Social media companies are bracing for Supreme Court arguments on Monday that could fundamentally alter how the platforms police their sites," *New York Times,* February 25, 2024; and Adam Liptak, "The Supreme Court seemed skeptical on laws in Florida and Texas," *Id.* February 26, 2024.)

Like constitutional and preemption questions, there is no obvious or certain answer as to whether this bill violates the First Amendment or Section 230. The Court may provide some insight soon enough.

Proposed Author Amendments. The author will take the following amendments to the definitions section of the bill:

(a) ***"Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.***

(b) (1) "Elections official" means any of the following persons, but only in their capacity as a person charged with holding or conducting an election, conducting a canvass, assisting with the holding or conducting of an election or a canvas, or performing another duty related to administering the provisions of this code:

(A) An elections official as defined in Section 320.

(B) The Secretary of State and their staff.

(C) A temporary worker, poll worker, or member of a precinct board.

(D) Any other person charged with holding or conducting an election, conducting a canvass, assisting with the holding or conducting of an election or a canvas, or performing another duty related to administering the provisions of this code.

(2) The requirements of this chapter relating to content portraying an elections official apply only if the large online platform knows or should know that the person is an elections official.

(c) ~~(b)~~ "Election processes" means any government process related to an election, including, but not limited to, elections, candidates, vote counting, redistricting, and proceedings or processes of the electoral college.

(d) ~~(c)~~ (1) "Materially deceptive and digitally modified or created content" means an image or an audio or video recording or other digital content, including a chatbot, that has been intentionally manipulated such that all of the following conditions are met:

(A) (i) The digital content is the product of digital manipulation, ***including, but not limited to, artificial intelligence***, ~~artificial intelligence, or machine learning, including deep learning techniques, that merges, combines, replaces, or superimposes content onto an image or an audio or video recording, creating an image or an audio or video recording that appears authentic, or that otherwise generates an inauthentic image or an audio or video recording~~ that appears authentic, ~~and that~~ ***but*** contains a false portrayal of any of the following: a candidate for elective office, elected official, elections official, voting machine, ballot, voting site, other property or equipment related to an election, or elections process.

(ii) For purposes of this subdivision, "false portrayal" means the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if they were hearing or seeing ~~the unaltered, original~~ ***an authentic*** version of the content.

(B) The person or entity who attempted to post or send, or who did post or send, the content did so knowing the portrayal was false, or did so with reckless disregard for whether the portrayal was false. If the content is intentionally manipulated and contains a false portrayal as specified in subparagraph (A), there shall be a rebuttable presumption that the person or entity knew the portrayal was false or that they acted with reckless disregard for whether the portrayal was false.

(2) "Materially deceptive and digitally modified or created content" does not include any image or audio or video recording that contains only minor modifications that do not lead to significant changes to the perceived contents or meaning of the content. Minor changes include changes to the brightness or contrast of images, removal of background noise in audio, and other minor changes that do not impact the content of the image or audio or video recording.

(e) ~~(d)~~ "Large online platform" means a public-facing internet website, web application, or digital application, including a social network, video sharing platform, advertising network, or search engine that had at least 1,000,000 California users during the preceding 12 months.

***ARGUMENTS IN SUPPORT**:* The sponsor of this bill – The California Initiative for Technology and Democracy (CITED) – writes in support of AB 2655:

> California and the nation are entering the first-ever generative artificial intelligence (AI) election, in which disinformation powered by generative AI will pollute our information ecosystems like never before. . . Those trying to influence campaigns – conspiracy theorists, foreign states, online trolls, and candidates themselves – are already creating and distributing election-threatening deepfake images, audio, and video content in the US and around the world. . . Examples of this occurring in U.S. elections include Ron Desantis using AI-generated images to attack his opponent in his presidential run, foreign states caught attempting to influence American politics through social media, and just this month, a supporter of former President Trump creating a deepfake image of Trump with Black Americans designed to persuade Black voters to support Trump. These examples demonstrate the power of generative AI-fueled disinformation to skew election results and weaken our faith in our democracy.
>
> AB 2655 strikes the right balance by seeking to ban, for a strictly limited time before and after elections, the online spread of the worst deepfakes and disinformation maliciously intended to prevent voters from voting or getting them to vote erroneously based on fraudulent content. . . AB 2655's approach is narrowly tailored and does not extend the law to hot button controversies or inflammatory claims – it does not ask social media platforms to adjudicate controversial opinions post by post. It simply stops the use of obviously, demonstrably untrue and provably false content meant to impermissibly influence our elections at peak election times.

***ARGUMENTS IN OPPOSITION**:* Opponents of AB 2655 contend that the bill is unnecessary, unwise, unconstitutional, or some combination thereof. A coalition of groups representing the technology and information industry (industry opponents) contend that responsible digital service providers already "take aggressive steps to moderate dangerous and illegal content, consistent with their terms of service. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review." For example, industry opponents point to the several online businesses that voluntarily participate in "the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices to ensure a safer and more trustworthy internet, and have recently reported on the efforts to implement these commitments."

Industry opponents believe that AB 2655 falsely assumes that online platforms "definitively know whether any particular piece of content has been manipulated in such a way that is defined under the bill. While digital services may employ tools to identify and detect these materials with some degree of certainty, it is an evolving and imperfect science in its current form. AB 2655 also presumes that online platforms are an appropriate arbiter of deciding what constitutes accurate election information. However, most digital services are not equipped with the tools or expertise to make such judgments."

In addition to these practical and operational concerns, industry opponents also question the effectiveness of the bill's approach. For example, they point out that the bill only applies to the largest online platforms, specifically those with at least one million California users. Therefore the bill would not include platforms like Truth Social or Parler (which may relaunch this year) even though they are the ones that produce most of the concern. Opponents also point to the "sweeping" enforcement provisions, most notably the provision that allows "any California

resident" to notify the platform of content that, in the resident's opinion, should have been blocked or labeled. The bill, opponents note, would allow this resident "to bring a civil action against a large online platform if the platform has not responded within 36 hours or if the reporting resident disagrees with the platform's response." Confronted with such a restricted timeline and the threat of a civil action, the opponents contend, platforms will "remove significantly more content, including content that has *accurate* election information and content that is not materially deceptive."

While industry opponents concentrate on problems of implementation and effectiveness, ACLU California Action focuses on the bill's constitutional problems. ACLU agrees that protecting "election integrity is a weighty governmental interest," but under the First Amendment, "that interest may be accomplished . . . only by means that are narrowly tailored." ACLU points to ample First Amendment case law holding that discussion "of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution." Quoting *Buckley v. Valeo* (1976), ACLU writes that the First Amendment affords "the broadest protection to such political expression in order to assure the unfettered interchange of ideas for the bringing about of political and social changes desired by the people," and, quoting *New York Times v Sullivan* (1964), ACLU notes that debate on public issues must remain "uninhibited, robust, and wide-open." Moreover, ACLU notes, the First Amendment affords protection "to even allegedly false statements about public officials and public figures." ACLU fears that faced with "the prospect of vetting millions of different posts to determine if they are 'materially deceptive and digitally modified or created,' many platforms may instead choose to aggressively censor or prohibit speech out of caution, including speech by candidates or relating to entire political topics." Citing *Brown v. Entertainment Merchants Association* (2011) and *Burstyn v Wilson* (1952), ACLU concludes that however much the technology may change, "the basic principles of freedom of speech and the press" do not vary with each new medium of communication. ACLU believes that the provisions of AB 2655, as currently drafted, "threaten to intrude on those rights and deter that vital speech."

REGISTERED SUPPORT / OPPOSITION:

Support

California Initiative for Technology & Democracy (sponsor)
AFSCME California
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
Bay Rising
California Clean Money Campaign
California Initiative for Technology & Democracy, a Project of California Common CAUSE
California State Sheriffs' Association
California Voter Foundation
Chinese Progressive Association
Courage California
Disability Rights California
Hmong Innovating Politics
Indivisible CA Statestrong
Inland Empire United
League of Women Voters of California

Partnership for the Advancement of New Americans
SEIU California
The Partnership for the Advancement of New Americans
Verified Voting

Opposition

ACLU California Action
Chamber of Progress
Computer and Communications Industry Association
Electronic Frontier Foundation
Internet.Works
NetChoice
Software & Information Industry Association
TechNet

Opposition unless amended

Oakland Privacy

Analysis Prepared by: Tom Clark / JUD. / (916) 319-2334

EXHIBIT 10

SENATE COMMITTEE ON ELECTIONS AND CONSTITUTIONAL AMENDMENTS

Senator Catherine Blakespear, Chair
2023 - 2024 Regular

Bill No:	AB 2655	**Hearing Date:**	6/18/24
Author:	Berman		
Version:	6/11/24		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Scott Matsumoto		

Subject: Defending Democracy from Deepfake Deception Act of 2024

DIGEST

This bill requires an online platform with at least one million California users to block, prevent the posting or spread of, or to label any elections-related content deemed to be materially deceptive if certain conditions are met.

ANALYSIS

Existing law:

1) Prohibits anyone from, until January 1, 2027, distributing within 60 days of an election materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

2) Prohibits anyone from, beginning January 1, 2027, producing, distributing, publishing, or broadcasting campaign material that contains a superimposed image of a candidate unless the campaign material includes a disclaimer that the picture is an inaccurate representation of fact.

This bill:

1) Requires a large online platform (platform) using state-of-the-art, best available tools to detect materially deceptive content, to block and prevent the posting or sending of materially deceptive content related to elections if:

   a) The content is posted between 120 days before the election and through Election Day (or through the 60th day after the election in the case of content that depicts or pertains to elections officials) if the platform knows or should know the content portrays any of the following:

      i) A candidate for elective office portrayed as doing or saying something they did not do or say and is reasonably likely to harm the reputation or electoral prospects of a candidate.

      ii) An elections official portrayed as doing or saying something in connection with their elections-related duties they did not do or say and is reasonably

likely to falsely undermine confidence in the outcome of one or more election contests.

iii) An elected official portrayed as doing or saying something that influences the election that they did not do or say and is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

b) The person or entity who created the materially deceptive content did so knowing it was false or with reckless disregard for the truth. There shall be a rebuttable presumption the person or entity knew the materially deceptive content was false or acted with reckless disregard for the truth if the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if hearing or seeing an authentic version of the content.

2) Requires platforms to develop and implement procedures for labeling content as inauthentic, fake, or false if the content is posted outside of the time period described in (1) or appears within an advertisement or election communication not subject to (1). This would apply in cases where the person or entity created the content knowing it was false, and the platform knew or should have known that the content was suppose to meet the labeling requirements prescribed by this bill.

3) Requires platforms to provide a way for Californians to report content that was not properly blocked or labeled to the platform. Allows a candidate, elected official, or elections official who reported content to the platform but does not receive a response in 36 hours or disagrees with the response – as well as the Attorney General (AG), a district attorney, or a city attorney – to seek injunctive or other equitable relief against a platform to compel compliance with this bill.

4) Provides this bill does not apply to satire or parody or to a regularly-published online periodical that publishes materially deceptive content that contains a clear disclosure that the content is not an accurate representation of reality.

5) Defines the following terms for the purposes of this bill:

a) “Deepfake” to mean audio or visual media that is digitally created or modified such that it would falsely appear to a reasonable person to be an authentic record of the actual speech or conduct of the individual depicted in the media;

b) “Materially deceptive content” to mean audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content depicted in the media; and

c) “Large online platform” to mean a public-facing internet website, web application, or digital application that had at least one million California users in the preceding 12 months.

BACKGROUND

Manipulated Media in Campaign Communications. The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. During its inaugural session in 1850, the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for."

California law today includes various provisions criminalizing deceptive tactics that undermine election integrity or interfere with voters' ability to participate in elections. This includes laws that prohibit the distribution of false and misleading information about qualifications to vote or about the days, dates, times, and places where voting may occur; prohibit the misleading use of government seals in campaign literature; and prohibit coercing or deceiving people into voting in a way that was inconsistent with the person's intent.

Artificial Intelligence (AI) and Elections. On June 4, 2024, the Senate Committee on Elections and Constitutional Amendments and the Assembly Committee on Elections held a joint information hearing focusing on AI and elections.

The purpose of the hearing was to inform and assist the Legislature in making informed decisions on legislation related to AI-generated and altered content. It became evident that the ease with which people can create and spread mis- and disinformation creates a world where many people may have trouble determining what is fact and what is fiction. The development of increasingly advanced AI tools has made once time-consuming activities much easier to complete, while also enabling the completion of tasks that are otherwise too complex for humans to tackle alone.

State Action. In 2018, the Legislature approved and Governor Brown signed AB 3075 (Berman), Chapter 241, Statutes of 2018 to establish the Office of Elections Cybersecurity (OEC) in the Secretary of State's (SOS) office. The OEC has two primary missions. First, it is responsible for coordinating efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation.

In 2019, the Legislature approved and Governor Newsom signed AB 730 (Berman), Chapter 493, Statutes of 2019. AB 730 sought to address concerns that deepfake technology could be used to spread misinformation in political campaigns. Legislative analyses of AB 730 described "deepfake technology" as software capable of producing a realistic looking video of someone saying or doing something they did not actually say or do.

AB 730 prohibits anyone from distributing deceptive audio or visual media with actual malice and the intent to injure a candidate's reputation or to deceive a voter, unless the media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, but also to any intentional manipulation of audio or visual images where a reasonable person would be misled into believing it was authentic. Notably, AB 730 focused on materially deceptive representations of candidates, and not on deceptive media of other aspects of the electoral process.

AB 730 included a January 1, 2023 sunset date, but in 2022, the Legislature approved AB 972 (Berman), Chapter 745, Statutes of 2022, to extend the sunset date to January 1, 2027.

Tech Accord to Combat Deceptive Use of AI in 2024. In February 2024, 20 technology companies signed the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections." This set of commitments seeks to combat harmful AI-generated content meant to deceive voters. The signatories included Adobe, Amazon, Anthropic, Arm, ElevenLabs, Google, IBM, Inflection AI, LinkedIn, McAfee, Meta, Microsoft, Nota, OpenAI, Snap Inc., Stability AI, TikTok, Trend Micro, Truepic, and X.

The signatories committed to taking the following steps through this year:

1) Develop and implement technology to mitigate risks related to deceptive AI content.
2) Assess and better understand the risks presented by deceptive AI election content.
3) Seek ways to detect the distribution of deceptive AI election content.
4) Seek to address deceptive AI election content.
5) Share best practices and explore pathways to share tools throughout the industry.
6) Provide transparency to the public.
7) Continue to engage with stakeholders to better understand the global risk landscape.
8) Support efforts to raise public awareness regarding deceptive AI election content.

Other States. According to the National Conference of State Legislatures, 16 states (Alabama, Arizona, California, Colorado, Florida, Idaho, Indiana, Michigan, Minnesota, Mississippi, New Mexico, Oregon, Texas, Utah, Washington, and Wisconsin) enacted legislation designed to address deceptive media, including but not limited to, AI.

COMMENTS

1) According to the Author: "AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in technology make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy."

2) First Amendment Considerations. The First Amendment to the United States (US) Constitution provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

   This bill seeks to regulate the distribution by online platforms of media containing intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California Constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

   This bill targets deceptive content that could undermine the public's trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds would likely hinge on whether the court found this bill's provisions to be narrowly tailored.

3) Banned Sometimes, Labeled Other Times. This bill requires online media platforms with more than one million users to detect materially deceptive content, block, and prevent the posting or distribution of materially deceptive content related to elections from 120 days before an election and, in some cases, 60 days after an election.

   However, for the other six to eight months of the year, the platforms would only have to label the materially deceptive content as such.

   The Committee may wish to consider whether this distinction is appropriate and why, if content is materially deceptive, the content should not be banned entirely from the platform, regardless of how close to an election such content is posted or displayed.

4) Election Timing. This bill requires platforms to block content beginning 120 days before an election and ending as many as 60 days after the election. As drafted, this would include any election in California. As a result, in counties where there are large numbers of elections (statewide, legislative, and congressional elections are held in every even-numbered year and many cities hold local elections in odd-numbered years), platforms may be blocking content almost constantly in order to ensure compliance with the provisions of this bill.

5) Double Referral. If approved by this committee, AB 2655 will be referred to the Committee on Judiciary for further consideration.

RELATED/PRIOR LEGISLATION

AB 2355 (W. Carrillo) of 2024 requires a campaign committee that creates, originally publishes, or originally distributes a political advertisement to include a disclosure stating that the audio, image, or video was generated or substantially altered using AI. AB 2355 is being considered by this committee.

AB 2839 (Pellerin) of 2024 prohibits the distribution of campaign advertisements and other election communications containing materially deceptive and digitally altered or created images or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign. AB 2839 is being considered by this committee.

PRIOR ACTION

Assembly Floor:	56 - 1
Assembly Appropriations Committee:	11 - 1
Assembly Elections Committee:	6 - 1

POSITIONS

Sponsor: California Initiative for Technology & Democracy

Support: Disability Rights California
League of Women Voters in California

Oppose: ACLU California Action
California Chamber of Commerce
Computer and Communications Industry
NetChoice
Software and Information Industry Association
TECHNET

-- END --

EXHIBIT 11

SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 2655 (Berman)
Version: June 11, 2024
Hearing Date: July 2, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Defending Democracy from Deepfake Deception Act of 2024

DIGEST

This bill establishes the Defending Democracy from Deepfake Deception Act of 2024, which requires a large online platform to block the posting or sending of materially deceptive and digitally modified or created content related to elections, during specified periods before and after an election. It requires these platforms to label certain additional content inauthentic, fake, or false during specified periods before and after an election and to provide mechanisms to report such content.

EXECUTIVE SUMMARY

The rapid advancement of AI technology, specifically the wide-scale introduction of generative AI models, has made it drastically cheaper and easier to produce synthetic content – audio, images, text, and video recordings that are not real, but that are so realistic that they are virtually impossible to distinguish from authentic content, including so-called "deepfakes." In the context of election campaigns, such deepfakes can be weaponized to deceive voters into thinking that a candidate said or did something which the candidate did not, or otherwise falsely call election results into question. A series of bills currently pending before this Committee attempt to address these issues by restricting or labeling AI-altered or –generated content. However, this bill specifically targets social media platforms and such materially deceptive content on their platforms, requiring platforms to block and prevent it, label it, and provide mechanisms for reporting it.

The bill is sponsored by the California Initiative for Technology & Democracy. It is supported by various organizations, including the League of Women Voters of California and Disability Rights California. It is opposed by Oakland Privacy and various industry associations, including TechNet. The bill passed out of the Senate Elections and Constitutional Amendments Committee on a 6 to 1 vote.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides that "Congress shall make no law… abridging the freedom of speech..." (U.S. Const., amend. 1.)

2) Applies the First Amendment to the states through operation of the Fourteenth Amendment. (*Gitlow v. New York* (1925) 268 U.S. 652; *NAACP v. Alabama* (1925) 357 U.S. 449.)

3) Provides, in federal law, that a provider or user of an interactive computer service shall not be treated as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230(c)(1).)

4) Provides that a provider or user of an interactive computer service shall not be held liable on account of:
   a. any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
   b. any action taken to enable or make available to information content providers or others the technical means to restrict access to such material. (47 U.S.C. § 230(c)(2).)

5) Provides that no provider or user of an interactive computer service shall be treated for liability purposes as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230.)

6) Defines "materially deceptive audio or visual media" as an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:
   a. The image or audio or video recording would falsely appear to a reasonable person to be authentic.
   b. The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording. (Elec. Code § 20010(e).)

7) Prohibits a person, committee, or other entity from distributing with actual malice materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate within 60 days of an election at which a candidate for elective office will appear on the ballot, as specified and unless specified conditions are met. (Elec. Code § 20010(a).)

8) Exempts audio or visual media that includes a disclosure stating: "This _____ has been manipulated." Requires the blank in the disclosure to be filled with a term that most accurately describes the media, as specified. Requires the following disclosures for visual and audio-only media:
   a. For visual media, the text of the disclosure shall appear in a size that is easily readable by the average viewer and no smaller than the largest font size of other text appearing in the visual media. If the visual media does not include any other text, then the disclosure shall appear in a size that is easily readable by the average viewer. Requires, for visual media that is video, the disclosure to be displayed throughout the duration of the video.
   b. For audio-only media, the disclosure shall be read in the clearly spoken manner and in a pitch that can be easily heard by the average listener, at the beginning of the audio, at the end of the audio, and, if the audio is greater than two minutes in length, interspersed within the audio at intervals of not greater than two minutes each. (Elec. Code § 20010(b).)

9) Permits a candidate for elective office whose voice or likeness appears in a materially deceptive audio or visual media distributed in violation of the above provisions, to seek injunctive or other equitable relief prohibiting the distribution of audio or visual media in violation. (Elec. Code § 20010(c)(1).)

10) Permits a candidate for elective office whose voice or likeness appears in materially deceptive audio or visual media distributed in violation of the above provisions to bring an action for general or special damages against the person, committee, or other entity that distributed the materially deceptive audio or visual media, as specified. Requires the plaintiff to bear the burden of establishing the violation through clear and convincing evidence in any civil action alleging a violation, as specified. (Elec. Code § 21101(c)(2).)

This bill:

1) Establishes the Defending Democracy from Deepfake Deception Act of 2024.

2) Requires a large online platform, using state-of-the-art, best available tools to detect materially deceptive content, to develop and implement procedures for blocking and preventing, and, if the platform knows or should know that the materially deceptive content meets the requirements hereof, to block and prevent

the posting or sending of any materially deceptive content, if all of the following conditions are met:

a) The content is posted or sent during a period beginning 120 days before the election and through the day of the election. For content that depicts or pertains to elections officials, this period shall extend to the 60th day after the election.
b) The materially deceptive content is any of the following:
    i. A candidate for elective office portrayed as doing or saying something that the candidate did not do or say and that is reasonably likely to harm the reputation or electoral prospects of a candidate.
    ii. An elections official portrayed as doing or saying something in connection with the performance of their elections-related duties that the elections official did not do or say and that is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.
    iii. An elected official portrayed as doing or saying something that influences the election that the elected official did not do or say and that is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.
c) The person or entity who created the materially deceptive content did so knowing it was false or with reckless disregard for the truth. There shall be a rebuttable presumption that the person or entity knew the materially deceptive content was false or acted with reckless disregard for the truth if the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if hearing or seeing an authentic version of the content.

3) Requires, notwithstanding the above, a large online platform to allow a candidate for elective office, during a period beginning 120 days before the election and through the day of the election, to portray themself as doing or saying something that the candidate did not do or say, but only if the digital content includes a disclosure meeting specified conditions and states the following: "This [category of content] has been manipulated."

4) Requires a large online platform, using state-of-the-art, best available tools to detect materially deceptive content to develop and implement procedures for labeling such content as inauthentic, fake, or false if all of the following conditions are met:
    a) The materially deceptive content is either of the following:
        i. Meets the standards set above, but is posted or sent outside the applicable time period.
        ii. Appears within an advertisement or election communication and is not subject to the above.

b) The person or entity who created the materially deceptive content did so knowing it was false or with reckless disregard for the truth. There shall be a rebuttable presumption that the person or entity knew the materially deceptive content was false or acted with reckless disregard for the truth if the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if hearing or seeing an authentic version of the content.
c) The large online platform knows or should know that the materially deceptive content meets the requirements of this section.

5) Specifies required functionality of the label above and states the labeling requirement applies during redistricting and during a period from one year before the election through election day. If the content involves elections officials, the electoral college process, the canvass of the vote, or election-related equipment or property, the time period is extended 60 days beyond the election.

6) Requires a large online platform to provide an easily accessible way for California residents to report to that platform content subject to the above provisions that was not blocked or labeled as required. The online platform shall respond to the person who made the report, within 36 hours of the report, describing any action taken or not taken by the online platform with respect to the content.

7) Authorizes a candidate for elective office, elected official, or elections official who has made a report and who either has not received a response within 36 hours or disagrees with the response, as well as the Attorney General or any district attorney or city attorney, to seek injunctive or other equitable relief against the online platform to compel compliance. The plaintiff shall bear the burden of establishing the violation through clear and convincing evidence. The court is required to award a prevailing plaintiff reasonable attorney's fees and costs. Such actions are given precedence in accordance with Section 35 of the Code of Civil Procedure.

8) Clarifies that it applies to materially deceptive content, regardless of the language used in the content. If the language used is not English, the required disclosure and label must appear in the language used as well as in English.

9) Requires a large online platform that blocks or labels any materially deceptive content to maintain a copy of the digital content for a period of not less than five years from the election and shall make such digital content available to the Secretary of State, the Fair Political Practices Commission, and researchers, if requested.

10) Exempts from the scope of the bill the following:
    a) A regularly published online newspaper, magazine, or other periodical of general circulation that routinely carries news and commentary of general interest, and that publishes any materially deceptive content that an online platform is required to block or label based on this chapter, if the publication contains a clear disclosure that the materially deceptive content does not accurately represent any actual event, occurrence, appearance, speech, or expressive conduct.
    b) Materially deceptive content that constitutes satire or parody.

11) Includes findings and declarations and a severability clause.

12) Defines the relevant terms, including:
    a) "Materially deceptive content" means audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content depicted in the media.
    b) "Large online platform" means a public-facing internet website, web application, or digital application, including a social network, video sharing platform, advertising network, or search engine that had at least 1,000,000 California users during the preceding 12 months.

COMMENTS

1. Blurring reality: AI-generated content

Generative AI is a type of artificial intelligence that can create new content, including text, images, code, or music, by learning from existing data. Generative AI models can produce realistic and novel artifacts that resemble the data they were trained on, but do not copy it. For example, generative AI can write a poem, draw a picture, or compose a song based on a given prompt or theme. Generative AI enables users to quickly generate new content based on a variety of inputs. Generative AI models use neural networks to identify the patterns and structures within existing data to generate new and original content.

The world has been in awe of the powers of this generative AI since the widespread introduction of AI systems such as ChatGPT. However, the capabilities of these advanced systems leads to a blurring between reality and fiction. The Brookings Institution lays out the issue:

> Over the last year, generative AI tools have made the jump from research prototype to commercial product. Generative AI models like OpenAI's ChatGPT and Google's Gemini can now generate realistic text and images that are often indistinguishable from human-authored content, with

> generative AI for audio and video not far behind. Given these advances, it's no longer surprising to see AI-generated images of public figures go viral or AI-generated reviews and comments on digital platforms. As such, generative AI models are raising concerns about the credibility of digital content and the ease of producing harmful content going forward.
>
> Against the backdrop of such technological advances, civil society and policymakers have taken increasing interest in ways to distinguish AI-generated content from human-authored content.[1]

One expert at the Copenhagen Institute for Future Studies estimates that should large generative-AI models run amok, up to 99 percent of the internet's content could be AI-generated by 2025 to 2030.[2] The problematic applications are seemingly infinite, whether it be deepfakes to blackmail or shame victims, false impersonations to commit fraud, or other nefarious purposes. Infamously, in January of this year, Taylor Swift was the victim of sexually explicit, nonconsensual deepfake images using AI that were widely spread across social media platforms.[3] Perhaps more disturbingly, a trend has emerged in schools of students creating such images: "At schools across the country, people have used deepfake technology combined with real images of female students to create fraudulent images of nude bodies. The deepfake images can be produced using a cellphone."[4] As more of the population becomes aware of the potential to realistically fake images, video, and text, some will use the skepticism that creates to challenge the authenticity of real content, a phenomena coined the "liar's dividend."[5]

Relevant here, AI and specifically generative AI can spread misinformation regarding elections with ease, both in California and across the world:

> Artificial intelligence is supercharging the threat of election disinformation worldwide, making it easy for anyone with a smartphone

---

[1] Siddarth Srinivasan, *Detecting AI fingerprints: A guide to watermarking and beyond* (January 4, 2024) Brookings Institution, https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/#:~:text=Google%20also%20recently%20announced%20SynthID,model%20to%20detect%20the%20watermark. All internet citations are current as of June 23, 2024.

[2] Lonnie Lee Hood, *Experts Say That Soon, Almost The Entire Internet Could Be Generated by AI* (March 4, 2022) The Byte, https://futurism.com/the-byte/ai-internet-generation.

[3] Brian Contreras, *Tougher AI Policies Could Protect Taylor Swift – And Everyone Else – From Deepfakes* (February 8, 2024) Scientific American, https://www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/.

[4] Hannah Fry, Laguna Beach High School investigates 'inappropriate' AI-generated images of students (April 2, 2024) Los Angeles Times, https://www.latimes.com/california/story/2024-04-02/laguna-beach-high-school-investigating-creation-of-ai-generated-images-of-students.

[5] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (July 14, 2018) 107 California Law Review 1753 (2019), https://ssrn.com/abstract=3213954.

> and a devious imagination to create fake – but convincing – content aimed at fooling voters.
>
> It marks a quantum leap from a few years ago, when creating phony photos, videos or audio clips required teams of people with time, technical skill and money. Now, using free and low-cost generative artificial intelligence services from companies like Google and OpenAI, anyone can create high-quality "deepfakes" with just a simple text prompt.
>
> A wave of AI deepfakes tied to elections in Europe and Asia has coursed through social media for months, serving as a warning for more than 50 countries heading to the polls this year.
>
> "You don't need to look far to see some people ... being clearly confused as to whether something is real or not," said Henry Ajder, a leading expert in generative AI based in Cambridge, England.
>
> The question is no longer whether AI deepfakes could affect elections, but how influential they will be, said Ajder, who runs a consulting firm called Latent Space Advisory.
>
> As the U.S. presidential race heats up, FBI Director Christopher Wray recently warned about the growing threat, saying generative AI makes it easy for "foreign adversaries to engage in malign influence."[6]

On that last note, in February of this year, voters in New Hampshire received robocalls that are purported to have used an AI voice resembling President Joe Biden advising them against voting in the presidential primary and saving their vote for the November general election.[7] The examples are endless:

> Former President Donald Trump, who is running in 2024, has shared AI-generated content with his followers on social media. A manipulated video of CNN host Anderson Cooper that Trump shared on his Truth Social platform on Friday, which distorted Cooper's reaction to the CNN town hall this past week with Trump, was created using an AI voice-cloning tool.

---

[6] Ali Swenson & Kelvin Chan, *Election disinformation takes a big leap with AI being used to deceive worldwide* (March 14, 2024) Associated Press, https://apnews.com/article/artificial-intelligence-elections-disinformation-chatgpt-bc283e7426402f0b4baa7df280a4c3fd.

[7] Em Steck & Andrew Kaczynski, *Fake Joe Biden robocall urges New Hampshire voters not to vote in Tuesday's Democratic primary* (January 22, 2024) CNN, https://www.cnn.com/2024/01/22/politics/fake-joe-biden-robocall/index.html.

> A dystopian campaign ad released last month by the Republican National Committee offers another glimpse of this digitally manipulated future. The online ad, which came after President Joe Biden announced his reelection campaign, and starts with a strange, slightly warped image of Biden and the text "What if the weakest president we've ever had was re-elected?"
>
> A series of AI-generated images follows: Taiwan under attack; boarded up storefronts in the United States as the economy crumbles; soldiers and armored military vehicles patrolling local streets as tattooed criminals and waves of immigrants create panic.
>
> "An AI-generated look into the country's possible future if Joe Biden is re-elected in 2024," reads the ad's description from the RNC.
>
> The RNC acknowledged its use of AI, but others, including nefarious political campaigns and foreign adversaries, will not, said Petko Stoyanov, global chief technology officer at Forcepoint, a cybersecurity company based in Austin, Texas. Stoyanov predicted that groups looking to meddle with U.S. democracy will employ AI and synthetic media as a way to erode trust.[8]

Legislatures across the country are pushing legislation that would address this looming threat.

2. Materially deceptive content in political advertisements

According to the author:

> AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in technology make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy.

[8] David Klepper & Ali Swenson, *AI-generated disinformation poses threat of misleading voters in 2024 election* (May 14, 2023) PBS News, https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election.

Unlike existing law or other bills pending before this Committee in this area, this bill seeks to place responsibility on large online platforms with regard to "materially deceptive content" regarding elections, placing a series of obligations on them. The bill defines "materially deceptive content" as audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content depicted in the media. "Large online platform" means a public-facing internet website, web application, or digital application, including a social network, video sharing platform, advertising network, or search engine that had at least 1,000,000 California users during the preceding 12 months.[9]

a. Preventing and blocking materially deceptive content

The bill requires platforms to develop and implement procedures for blocking and preventing, and, to block and prevent the posting or sending of, materially deceptive content, if the platform knows or should know that the materially deceptive content meets the requirements of the bill and certain conditions are met.

The materially deceptive content must portray one of the following. First is content portraying a candidate for elective office as doing or saying something they did not do or say and that is reasonably likely to harm the reputation or electoral prospects of a candidate. Or it must portray an elected official as doing or saying something that influences the election or an elections official as doing or saying something in connection with the performance of their elections-related duties that the official did not do or say and that is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

Second, the content must be posted or sent during a period beginning 120 days before the election and through the day of the election. For content that depicts or pertains to elections officials, this period shall extend to the 60th day after the election.

Finally, to trigger the requirement for platforms to block and prevent the content, the person or entity who created the content must have done so knowing it was false or with reckless disregard for the truth.

In any ensuing litigation, the bill establishes a rebuttable presumption that the person or entity knew the materially deceptive content was false or acted with reckless disregard for the truth if the content would cause a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if hearing or seeing an authentic version of the content.

[9] The author has agreed to an amendment that cross-references the existing definition for "social media platform, to replace the reference in the bill to "social network."

Carved out of this obligation is digital content that a candidate for elective office posts or shares that portrays themself as doing or saying something that they did not do, so long as there is a disclosure indicating that the content has been manipulated that meets certain specifications. However, not only is this content not subject to the requirement for a platform to block and prevent, but platforms are required to host such content and cannot prevent such material, with no exception for whether it violates the platforms terms and services. This provision similarly applies during the period starting 120 days before an election through election day.

b. Labeling materially deceptive content

Large online platforms are also required to develop and implement procedures for labeling materially deceptive content as inauthentic, fake, or false. This applies to such content that meets the requirements from the above section but falls outside of the specified time range or that does not meet the requirements but that appears within an advertisement or election communication. The person or entity who created the materially deceptive content must have also done so knowing it was false or with reckless disregard for the truth. The rebuttable presumption again applies. And, for this obligation to trigger, the large online platform must have known or should have known that the materially deceptive content meets these requirements.

The label must allow users to click or tap on it and to inspect all available provenance data about the content in an easy-to-understand format. The labeling requirement applies during specified time periods: (1) the period starting one year before the election through election day; (2) that period through the 60th day after the election, if it depicts or pertains to elections officials, the electoral college process, a voting machine, ballot, voting site, or other property or equipment related to an election, or the canvass of the vote; and (3) during a governmental process related to redistricting, as provided.

c. Retention requirement

Content that either requires such a label or that must be blocked and prevented from being posted and shared must be retained by the platform for not less than five years from the relevant election. Platforms must share the content, upon request, with the Secretary of State, the Fair Political Practices Commission, and researchers.

d. Reporting mechanism

Lastly, the bill requires a large online platform to provide an easily accessible way for California residents to report to that platform content subject to the above provisions that was not blocked or labeled as required. The online platform shall respond to the person who made the report, within 36 hours, describing any action taken or not taken by the online platform.

e. Enforcement

The bill provides standing to candidates, elected officials, or elections officials who have made reports but who have either not received a timely response or who disagree with it to bring an action for injunctive and other equitable relief. The Attorney General, district attorneys, and city attorneys are also so authorized. A prevailing plaintiff is entitled to attorneys' fees and costs. Such actions are given precedence in the courts.

However, plaintiffs in such actions are required to establish a violation by clear and convincing evidence.

3. Legal concerns

Concerns have been raised about whether the bill runs afoul of federal statutory and constitutional law. Namely, whether the bill is preempted by Section 230 of the Communications Decency Act, 47 U.S.C. § 230 and the First Amendment to the United States Constitution.

a. Section 230

Section 230 does not apply to the *users* of social media (or the internet generally), but rather applies to the *platforms themselves*. In the early 1990s, prior to the enactment of Section 230, two trial court orders—one in the United States District Court for the Southern District of New York, and New York state court—suggested that internet platforms could be held liable for allegedly defamatory statements made by the platforms' users if the platforms engaged in any sort of content moderation (e.g., filtering out offensive material).[10] In response, two federal legislators and members of the burgeoning internet industry crafted a law that would give internet platforms immunity from liability for users' statements, even if they might have reason to know that statements might be false, defamatory, or otherwise actionable.[11] The result—Section 230—was relatively uncontroversial at the time, in part because of the relative novelty of the internet and in part because Section 230 was incorporated into a much more controversial internet regulation scheme that was the subject of greater debate.[12]

---

[10] *See Cubby, Inc. v. Compuserve, Inc.* (S.D.N.Y. 1991) 776 F.Supp. 135, 141; *Stratton Oakmont v. Prodigy Servs. Co.* (N.Y. Sup. Ct., May 26, 1995) 1995 N.Y. Misc. LEXIS 229, *10-14. These opinions relied on case law developed in the context of other media, such as whether bookstores and libraries could be held liable for distributing defamatory material when they had no reason to know the material was defamatory. (*See Cubby, Inc.*, 776 F. Supp. at p. 139; *Smith v. California* (1959) 361 U.S. 147, 152-153.)

[11] Kosseff, The Twenty-Six Words That Created The Internet (2019) pp. 57-65.

[12] *Id.* at pp. 68-73. Section 230 was added to the Communications Decency Act of 1996 (title 5 of the Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56), which would have imposed criminal liability on internet platforms if they did not take steps to prevent minors from obtaining "obscene or indecent" material online. The Supreme Court invalidated the CDA, except for Section 230, on the basis that it violated the First Amendment. (*See Reno v. ACLU* (1997) 521 U.S. 844, 874.)

The crux of Section 230 is laid out in two parts. The first provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[13] The second provides a safe harbor for content moderation, by stating that no provider or user shall be held liable because of good-faith efforts to restrict access to material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[14]

Together, these two provisions give platforms immunity from any civil or criminal liability that could be incurred by user statements, while explicitly authorizing platforms to engage in their own content moderation without risking that immunity. Section 230 specifies that "[n]o cause of action may be brought and no liability may be imposed under any State law that is inconsistent with this section."[15] Courts have applied Section 230 in a vast range of cases to immunize internet platforms from "virtually all suits arising from third-party content."[16]

This bill provides for the potential liability of platforms for failing to block and prevent certain content from being posted or shared by users. If a user's content qualifies as materially deceptive, and other conditions are met, then the platform can be held liable for it.

Supporters point to the fact that monetary damages are not available and injunctive relief is essentially the only remedy available. The bill does allow for attorneys' fees and costs, which could be considered the type of liability that triggers Section 230's preemptive effect. The author has agreed to amendments that remove these remedies, leaving only injunctive relief. While courts, including the California Supreme Court, have found Section 230 immunity can extend to liability for solely injunctive relief, it is far from settled law in the country.[17]

In addition, the bill provide that if the platform engages in content moderation that restricts access to a candidate's deceptive portrayal of themselves (with the required disclosure and during the applicable time period), the platform can be held liable for that content moderation decision, regardless of the justification. As discussed below, the author has agreed to an amendment that removes this provision.

Ultimately, the bill is likely to face challenge on these grounds but these amendments work toward insulating the bill from such a challenge.

---

[13] *Id.*, § 230(c)(1).
[14] *Id.*, § 230(c)(1) & (2).
[15] *Id.*, § 230(e)(1) & (3).
[16] Kosseff, *supra*, fn. 13, at pp. 94-95; *see, e.g.*, *Doe v. MySpace Inc.* (5th Cir. 2008) 528 F.3d 413, 421-422; *Carfano v. Metrospalsh.com, Inc.* (9th Cir. 2003) 339 F.3d 1119, 1125; *Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327, 333-334.
[17] *Hassell v. Bird* (2018) 5 Cal. 5th 522, 547.

b. First Amendment

The First Amendment, as applied to the states through the Fourteenth Amendment, prohibits Congress or the states from passing any law "abridging the freedom of speech."[18] "[A]s a general matter, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."[19] However, while the amendment is written in absolute terms, the courts have created a handful of narrow exceptions to the First Amendment's protections, including "true threats,"[20] "fighting words,"[21] incitement to imminent lawless action,[22] defamation,[23] and obscenity.[24] Moreover, the First Amendment not only protects the right to speak, as a logical corollary it protects the "right to receive information and ideas."[25] Expression on the internet is given the same measure of protection granted to in-person speech or statements published in a physical medium.[26]

"Laws that burden political speech are subject to strict scrutiny, which requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest."[27] Content-based restrictions subject to strict scrutiny are "presumptively unconstitutional."[28] California courts have been clear that political expression in the context of campaigns of any manner should be given wide latitude:

> Hyperbole, distortion, invective, and tirades are as much a part of American politics as kissing babies and distributing bumper stickers and pot holders. Political mischief has been part of the American political scene since, at least, 1800.
>
> In any election, public calumny of candidates is all too common. "Once an individual decides to enter the political wars, he subjects himself to this kind of treatment. . . . [D]eeply ingrained in our political history is a tradition of free-wheeling, irresponsible, bare knuckled, Pier 6, political brawls." To endure the animadversion, brickbats and skullduggery of a given campaign, a politician must be possessed with the skin of a

[18] U.S. Const., 1st & 14th amends.
[19] *Ashcroft v. American Civil Liberties Union* (2002) 535 U.S. 564, 573.
[20] *Snyder v. Phelps* (2011) 562 U.S. 443, 452.
[21] *Cohen v. California* (1971) 403 U.S. 15, 20.
[22] *Virginia v. Black* (2003) 538 U.S. 343, 359.
[23] *R.A.V. v. St. Paul* (1992) 505 U.S. 377, 383.
[24] *Ibid.*
[25] *Stanley v Georgia* (1969) 394 U.S. 557, 564. Internal citations omitted
[26] *Reno v. ACLU* (1997) 521 U.S. 844, 870.
[27] *Citizens United v. FEC* (2010) 558 U.S. 310, 340. Internal citations omitted. It should be noted that while not controversial for the principle cited herein, this opinion is widely criticized for further tilting political influence toward wealthy donors and corporations.
[28] *Reed v. Town of Gilbert* (2015) 135 S.Ct. 2218, 2226 (*Reed*).

> rhinoceros. Harry Truman cautioned would-be solons with sage advice about the heat in the kitchen.
>
> Nevertheless, political campaigns are one of the most exhilarating phenomena of our democracy. They bring out the best and the worst in us. They allow candidates and their supporters to express the most noble and, lamentably, the most vile sentiments. They can be fractious and unruly, but what they yield is invaluable: an opportunity to criticize and comment upon government and the issues of the day.
>
> The candidate who finds himself or herself the victim of misconduct is not without a remedy. Those campaign tactics which go beyond the pale are sanctionable under FPPC laws.
>
> It is abhorrent that many political campaigns are mean-spirited affairs that shower the voters with invective instead of insight. The elimination from political campaigns of opprobrium, deception and exaggeration would shed more light on the substantive issues, resulting in a more informed electorate. It would encourage more able people to seek public office. But to ensure the preservation of a citizen's right of free expression, we must allow wide latitude.[29]

The United States Supreme Court has emphasized the extraordinary protection afforded to political speech:

> Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression in order "to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people." Although First Amendment protections are not confined to "the exposition of ideas," "there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs,… of course includ[ing] discussions of candidates…." This no more than reflects our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." In a republic where the people are sovereign, the ability of the citizenry to make informed choices among candidates for office is essential, for the identities of those who are elected will inevitably shape the course that we follow as a nation. As the Court observed in *Monitor Patriot Co. v. Roy*, 401 U.S. 265, 272 (1971), "it can hardly be doubted that the constitutional guarantee has its fullest and

[29] *Beilenson v. Superior Court* (1996) 44 Cal. App. 4th 944, 954-55. Internal citations omitted.

> most urgent application precisely to the conduct of campaigns for political office."[30]

This protection does not end where the truth of the speech does. "Although false statements of fact, by themselves, have no constitutional value, constitutional protection is not withheld from all such statements."[31] For instance, in the seminal opinion in *New York Times Co. v. Sullivan* (1964) 376 U.S. 254, 279-80, the court found the Constitution requires a rule that "prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' -- that is, with knowledge that it was false or with reckless disregard of whether it was false or not. The Supreme Court has expounded on this principle, providing nuance based on the knowledge of the speaker:

> Truth may not be the subject of either civil or criminal sanctions where discussion of public affairs is concerned. And since ". . . erroneous statement is inevitable in free debate, and . . . it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need . . . to survive' . . . ," only those false statements made with the high degree of awareness of their probable falsity demanded by *New York Times* may be the subject of either civil or criminal sanctions. For speech concerning public affairs is more than self-expression; it is the essence of self-government. The First and Fourteenth Amendments embody our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."
>
> The use of calculated falsehood, however, would put a different cast on the constitutional question. Although honest utterance, even if inaccurate, may further the fruitful exercise of the right of free speech, it does not follow that the lie, knowingly and deliberately published about a public official, should enjoy a like immunity. At the time the First Amendment was adopted, as today, there were those unscrupulous enough and skillful enough to use the deliberate or reckless falsehood as an effective political tool to unseat the public servant or even topple an administration. That speech is used as a tool for political ends does not automatically bring it under the protective mantle of the Constitution. For the use of the known lie as a tool is at once at odds with the premises of democratic government and with the orderly manner in which economic, social, or political change is to be effected. Calculated falsehood falls into that class of utterances which "are no essential part of any exposition of ideas, and are

[30] *Buckley v. Valeo* (1976) 424 U.S. 1, 14-15. Internal citations omitted.
[31] *People v. Stanistreet* (2002) 29 Cal. 4th 497, 505.

> of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. . . .” Hence the knowingly false statement and the false statement made with reckless disregard of the truth, do not enjoy constitutional protection.[32]

As stated, a restriction can survive strict scrutiny only if it uses the least-restrictive means available to achieve a compelling government purpose.[33] This bill implicates both the right to speak about elections, as well as the right to receive information regarding them. The bill is aimed at protecting the integrity of our elections, arguably a clearly compelling governmental interest. The question is whether the bill sufficiently tailors its provisions to effectuating that goal.

The bill seeks to prevent “materially deceptive content,” which is audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content depicted in the media, when it portrays candidates or elections officials doing or saying something they did not do or say. However, it does not target the person creating, posting, or sharing such content, but the platforms that host it. The bill attempts to tailor itself to the boundaries sketched out above. For instance, it imposes liability on the platforms only where they knew or should have known the content qualified as “materially deceptive content.” However, this falls short of the malice standard set forth in *Sullivan*, establishing something akin to a negligence standard instead.

The bill does impose a malice requirement but on the person or entity who created the content, requiring that they created it knowing it was false or with reckless disregard for the truth. However, liability is not imposed on the creator, nor even the one posting or sharing the content, but the social media platform allowing it on their platform. Further undercutting this element, there is a rebuttable presumption that the person who created it acted with malice if the content causes “a reasonable person to have a fundamentally different understanding or impression of the content than the person would have if hearing or seeing an authentic version of the content.” Therefore, the bill puts the onus on the platform to establish that the creator of the content, a person or entity the platform may not even have a relationship with or know, did not act with malice. Many of the relevant cases stress that the level of burden placed on a defendant to defend their political speech is a factor to consider. For instance, the following was stated in *Sullivan*:

> A rule compelling the critic of official conduct to guarantee the truth of all his factual assertions -- and to do so on pain of libel judgments virtually

[32] *Garrison v. Louisiana* (1964) 379 U.S. 64, 74-75. Internal citations omitted.
[33] *United States v. Playboy Entertainment Group* (2000) 529 U.S. 803, 813.

> unlimited in amount -- leads to a comparable "self-censorship." Allowance of the defense of truth, with the burden of proving it on the defendant, does not mean that only false speech will be deterred. Even courts accepting this defense as an adequate safeguard have recognized the difficulties of adducing legal proofs that the alleged libel was true in all its factual particulars.[34]

While the plaintiff is required to prove their case by clear and convincing evidence, the standards above place a burden on platforms to establish facts potentially well outside their bounds of knowing.

The California Initiative for Technology & Democracy (CITED), the sponsor of the bill, argues the case:

> AB 2655's approach is narrowly tailored and does not extend the law to hot button controversies or inflammatory claims – it does not ask social media platforms to adjudicate controversial opinions post by post. It simply stops the use of obviously, demonstrably untrue and provably false content meant to impermissibly influence our elections at peak election times. It is therefore respectful of the protections of the First Amendment and avoids concerns based on Section 230 of the Communications Decency Act.

Writing in opposition, ACLU California Action assesses the issue:

> Digitally modified content or content created using artificial intelligence (AI) tools is also entitled to [First Amendment] protections, unless the content falls within recognized First Amendment exceptions such as libel or fraud. The "novelty of deepfake technology and the speed with which it is improving" do not justify relaxing the stringent protections afforded to political speech by the First Amendment. The Supreme Court has held that "whatever the challenges of applying the Constitution to ever-advancing technology, 'the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary' when a new and different medium for communication appears."
>
> The law has long made clear that the First Amendment was intended to create a wide berth for political speech because it is the core of our democracy. The First Amendment provides robust protection for speech of all kinds. Speech that is false, confusing, or which presents content that some find abhorrent, nevertheless maintains its constitutional protections as a driver of free discourse. This remains so no matter what the

[34] *N.Y. Times Co. v. Sullivan*, at 279.

> technology used to speak. Unfortunately, the provisions of AB 2655 as currently drafted threaten to intrude on those rights and deter that vital speech.

In response to these concerns, the author has agreed to amendments that remove the provision that applies this malice standard to the creators of the content and instead more closely hews the platform's basis for liability to the malice standard, holding the large online platform liable only if it knows that the materially deceptive content meets the requirements of the bill or acts with a reckless disregard for the truth.[35]

As the bill also requires platforms to allow certain potentially misleading content to be posted, the bill could be found to implicate the First Amendment rights of platforms in their editorial discretion. Two laws in Florida and Texas that similarly seek to prevent platforms from taking down certain content have been challenged. The consolidated case has been argued before the United States Supreme Court and an opinion is forthcoming. The 11th Circuit Court of Appeals laid out its assessment of the First Amendment implications of such laws:

> Social-media platforms like Facebook, Twitter, YouTube, and TikTok are private companies with First Amendment rights and when they (like other entities) "disclos[e]," "publish[]," or "disseminat[e]" information, they engage in "speech within the meaning of the First Amendment." More particularly, when a platform removes or deprioritizes a user or post, it makes a judgment about whether and to what extent it will publish information to its users—a judgment rooted in the platform's own views about the sorts of content and viewpoints that are valuable and appropriate for dissemination on its site. As the officials who sponsored and signed S.B. 7072 [the challenged Florida law] recognized when alleging that "Big Tech" companies harbor a "leftist" bias against "conservative" perspectives, the companies that operate social-media platforms express themselves (for better or worse) through their content-moderation decisions. When a platform selectively removes what it perceives to be incendiary political rhetoric, pornographic content, or public-health misinformation, it conveys a message and thereby engages in "speech" within the meaning of the First Amendment.
>
> Laws that restrict platforms' ability to speak through content moderation therefore trigger First Amendment scrutiny.[36]

[35] This amendment includes corresponding changes in the labeling section of the bill.
[36] *NetChoice, LLC v. AG, Fla.* (11th Cir. 2022) 34 F.4th 1196, 1210. Internal citations and quotations omitted.

As constitutional analysis is subject to changing norms and interpretations, especially in the more political charged federal judiciary of the day, it is inherently difficult to predict whether this law will be struck down for violating the protections of the First Amendment. However, it is safe to say it will likely face legal challenge and arguably be vulnerable thereto.

In order to insulate the bill from such challenge, the author has agreed to an amendment that simply provides that the bill does not apply to a candidate's portrayal of themselves doing or saying something that the candidate did not do or say, where it includes the required disclosure.

c. Additional concerns

The bill raises a few additional concerns. First, the bill requires platforms to retain all content they have prevented or blocked or labeled pursuant to the bill. This forced retention of information raises some thorny legal issues and may interfere with existing consumer rights. For instance, the CCPA, as amended by the CPRA, grants a series of rights to consumers, including the right to delete information held by businesses. In addition, given that the retention provision is essentially a government mandate on private businesses to seize certain information of private individuals, Fourth Amendment issues arguably arise. Furthermore, the bill requires platforms to hand over the content to specified government entities and even "researchers," upon request. There is no limitation that there be evidence of a crime or some other justification and no probable cause necessary to be provided the information. In response, the author has agreed to an amendment to remove this retention requirement.

In addition, it is unclear what exactly is required by the bill's requirement to block or prevent the *sending* of materially deceptive content. This could be read to apply to private messaging features of these platforms, essentially requiring platforms to scan private communications. This would raise serious privacy concerns. In response, the author has agreed to amendments that remove the "sending" element of the bill.

In addition, groups in opposition raise concerns that the bill presupposes a level of sophistication for technology that can detect AI-generated or manipulated content that simply does not exist. A coalition of industry associations, including NetChoice writes in opposition:

> AB 2655 appears to be based on the false assumption that online platforms definitively know whether any particular piece of content has been manipulated in such a way that is defined under the bill. While digital services may employ tools to identify and detect these materials with some degree of certainty, it is an evolving and imperfect science in its current form. AB 2655 also presumes that online platforms are an appropriate arbiter of deciding what constitutes accurate election

> information. However, most digital services are not equipped with the tools or expertise to make such judgments.

Oakland Privacy writes in opposition:

> The bill language offers that a technology company should be the judge, jury and executioner, although it may be unclear if the content is or is not generative AI-created and what role generative AI played in the content. It is unclear to us how any technology platform can be expected to know everything that every candidate in every city, county, state and federal election said and everywhere they went. Not to mention every other elected official in the state. If this is the basis for the removal of content by a technology platform, it is highly speculative and largely dependent on reports to the platform, which may be inaccurate, politically motivated, or malicious.
> We appreciate amendments to raise the bar for the knowledge level of online platforms. But we continue to have concerns on the other side of the spectrum: the removal of content that should not be removed and may well impact election results.
>
> In other words, the bill language is relying on two imprecise measures: technically scanning content for synthetic material with highly inaccurate tools, and real-life reports from the public, candidates and election officials and campaigns or chaos actors to power a broad censorship regime of blocking content. We cannot support that, even under the guise of defending democracy.

The opposition coalition also takes issue with the enforcement mechanism:

> [B]ecause AB 2655 is focused on enforcement against covered platforms and not the actors who are intentionally seeking to materially deceive other consumers, it is unlikely to meaningfully reduce the amount of election mis- and disinformation hosted online. While the June 11 amendments appear to attempt to address this issue, we do not believe the new language effectively resolves our concerns. For example, the bill now allows for a "rebuttable presumption" but still fails to effectively address and hold accountable the purveyors of deceptive content.

4. Support

CITED, the sponsor of the bill, writes:

> Those trying to influence campaigns – conspiracy theorists, foreign states, online trolls, and candidates themselves – are already creating and

> distributing election-threatening deepfake images, audio, and video content in the US and around the world. This threat is not imaginary: generative AI has been used in various ways – most of them deeply deceptive – to influence the national elections in Slovakia, Bangladesh, Argentina, Pakistan, and elsewhere, including in our own country. Examples of this occurring in U.S. elections include Ron Desantis using AI-generated images to attack his opponent in his presidential run, foreign states caught attempting to influence American politics through social media, and just this month, a supporter of former President Trump creating a deepfake image of Trump with Black Americans designed to persuade Black voters to support Trump.
>
> These examples demonstrate the power of generative AI-fueled disinformation to skew election results and weaken our faith in our democracy. We cannot let it undermine our elections here in California, and we are grateful you are leading the effort to try to stop it.
>
> AB 2655 strikes the right balance by seeking to ban, for a strictly limited time before and after elections, the online spread of the worst deepfakes and disinformation maliciously intended to prevent voters from voting or getting them to vote erroneously based on fraudulent content. The bill also requires that other fake online content related to elections and elections processes (such as redistricting), which is also designed to undermine election procedures and democratic institutions, must be labeled as fake, again just for a limited time. The bill only applies to the largest online platforms with the greatest reach of potential election disinformation, and we believe it is fully implementable today based on tools these companies already possess. The companies covered by the bill's requirements are all already subject to similar requirements under the European Union's Digital Services Act, which is designed to, among other things, crack down on election interference.

A coalition of groups in support, including the American Federation of State, County, and Municipal Employees (AFSCME) and NextGen CA, write:

> AB 2655 seeks to solve these problems by, for a limited time before and after elections, banning the online spread of the worst of the deepfakes and disinformation meant to prevent voters from voting or to deceive them based on fraudulent content, and requiring that other fake content to be labeled as such. The approach leans heavily on increasing transparency, with bans used at only the highest-leverage moments, making it narrowly tailored. Additionally, it does not extend the law to hot button controversies or inflammatory claims – just the depiction of demonstrably untrue and provably false content meant to impermissibly

> influence our elections, at peak times – and is therefore implementable and respectful of the protections of the First Amendment.

Writing in support, the Northern California Recycling Association explains the need for the bill:

> California is entering its first-ever generative Artificial Intelligence (AI) election, in which disinformation powered by generative AI would and will pollute our information ecosystems like never before. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in AI make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy.

SUPPORT

California Initiative on Technology and Democracy (sponsor)
AFSCME California
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans and Pacific Islanders for Civic Empowerment
Asian Law Alliance
Bay Rising
Board of Supervisors for the City and County of San Francisco
California Clean Money Campaign
California Environmental Voters
California State Sheriff's Association
California Voter Foundation
Center for Countering Digital Hate
Chinese Progressive Association
City and County of San Francisco Board of Supervisors
Courage California
Disability Rights California
Hmong Innovating Politics
Inland Empire United
League of Women Voters of California
Move (mobilize, Organize, Vote, Empower) the Valley
Nextgen California
Northern California Recycling Association
Partnership for the Advancement of New Americans
SEIU California
Techequity Action

Verified Voting
Young People's Alliance
Youth Power Project

OPPOSITION

ACLU California Action
California Chamber of Commerce
Computer & Communications Industry Association
Electronic Frontier Foundation
Internet Works
Netchoice
Oakland Privacy
Software & Information Industry Association
Technet

RELATED LEGISLATION

Pending Legislation:

SB 942 (Becker, 2024) establishes the California AI Transparency Act, requiring covered providers to create and make freely available an AI detection tool to detect content as AI-generated and to include disclosures in content generated by the provider's system. SB 942 is currently in the Assembly Judiciary Committee.

SB 970 (Ashby, 2024) ensures that media manipulated or generated by artificial intelligence (AI) technology is incorporated into the right of publicity law and criminal false impersonation statutes. The bill requires those providing access to such technology to provide a warning to consumers about liability for misuse. SB 970 was held on suspense in the Senate Appropriations Committee.

AB 2355 (Wendy Carrillo, 2024) requires committees that create, publish, or distribute a political advertisement that contains any image, audio, or video that is generated or substantially altered using artificial intelligence to include a disclosure in the advertisement disclosing that the content has been so altered. AB 2355 is currently in this Committee.

AB 2839 (Pellerin, 2024) prohibits a person, committee, or other entity from knowingly distributing an advertisement or other election communication that contains materially deceptive content, as defined and specified, with malice, except as provided, within 120 days of a California election, and in specified cases, 60 days thereafter. AB 2839 is currently in this Committee.

AB 2930 (Bauer-Kahan, 2024) requires, among other things, a deployer and a developer of an automated decision tool to perform an impact assessment for any automated

decision tool the deployer uses that includes, among other things, a statement of the purpose of the automated decision tool and its intended benefits, uses, and deployment contexts. AB 2930 requires a deployer to, at or before the time an automated decision tool is used to make a consequential decision, notify any natural person that is the subject of the consequential decision that an automated decision tool is being used to make, or be a substantial factor in making, the consequential decision and to provide that person with, among other things, a statement of the purpose of the automated decision tool. AB 2930 is currently in this Committee.

AB 3211 (Wicks, 2024) establishes the California Provenance, Authenticity and Watermarking Standards Act, which requires a generative AI system provider to take certain actions to assist in the disclosure of provenance data to mitigate harms caused by inauthentic content, including placing imperceptible and maximally indelible watermarks containing provenance data into content created by an AI system that the generative AI system provider makes available. AB 3211 also requires a large online platform, as defined, to, among other things, use labels to prominently disclose the provenance data found in watermarks or digital signatures in content distributed to users on its platforms, as specified. AB 3211 is currently in the Senate Appropriations Committee.

Prior Legislation: AB 730 (Berman, Ch. 493, Stats. 2019) prohibited the use of deepfakes depicting a candidate for office within 60 days of the election unless the deepfake is accompanied by a prominent notice that the content of the audio, video, or image has been manipulated. Additionally, AB 730 authorized a candidate who was falsely depicted in a deepfake to seek rapid injunctive relief against further publication and distribution of the deepfake.

PRIOR VOTES:

Senate Elections and Constitutional Amendments Committee (Ayes 6, Noes 1)
Assembly Floor (Ayes 56, Noes 1)
Assembly Appropriations Committee (Ayes 11, Noes 1)
Assembly Judiciary Committee (Ayes 9, Noes 0)
Assembly Elections Committee (Ayes 6, Noes 1)
****

EXHIBIT 12

SENATE RULES COMMITTEE AB 2655

Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 2655
Author: Berman (D) and Pellerin (D), et al.
Amended: 8/23/24 in Senate
Vote: 21

SENATE ELECTIONS & C.A. COMMITTEE: 6-1, 6/18/24
AYES: Blakespear, Allen, Menjivar, Newman, Portantino, Umberg
NOES: Nguyen

SENATE JUDICIARY COMMITTEE: 9-2, 7/2/24
AYES: Umberg, Allen, Ashby, Caballero, Durazo, Laird, Roth, Stern, Wahab
NOES: Wilk, Niello

SENATE APPROPRIATIONS COMMITTEE: 5-2, 8/15/24
AYES: Caballero, Ashby, Becker, Bradford, Wahab
NOES: Jones, Seyarto

ASSEMBLY FLOOR: 56-1, 5/22/24 - See last page for vote

SUBJECT: Defending Democracy from Deepfake Deception Act of 2024

SOURCE: California Initiative for Technology & Democracy

DIGEST: This bill requires an online platform with at least one million California users to develop and implement procedures to identify and remove materially deceptive content if certain conditions are met.

Senate Floor Amendments of 8/23/24 remove local offices from the provisions of the bill, narrow the definition of an "elections official," modify the duties of large online platforms to identify and remove materially deceptive content, and specify that broadcasting stations are exempt from the provisions of the bill if there is an acknowledgement that the materially deceptive content does not represent any actual event. The amendments also contain technical and other clarifications. Finally, the amendments address chaptering issues with AB 2839 (Pellerin, 2024).

ANALYSIS:

Existing law:

1) Prohibits anyone from, until January 1, 2027, distributing within 60 days of an election materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.

2) Prohibits anyone from, beginning January 1, 2027, producing, distributing, publishing, or broadcasting campaign material that contains a superimposed image of a candidate unless the campaign material includes a disclaimer that the picture is an inaccurate representation of fact.

This bill:

1) Requires any large online platform (platform) using state-of-the-art techniques to identify and remove materially deceptive content related to elections in California if:

   a) The content is posted between 120 days before the election and through Election Day (or through the 60th day after the election in the case of content that depicts or pertains to elections officials), reported, and the materially deceptive content is any of the following:

      i) A candidate for elective office portrayed as doing or saying something they did not do or say and is reasonably likely to harm the reputation or electoral prospects of a candidate.

      ii) An elections official portrayed as doing or saying something in connection with their elections-related duties they did not do or say and is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

      iii) An elected official portrayed as doing or saying something that influences an election in California that they did not do or say and is reasonably likely to falsely undermine confidence in the outcome of one or more election contests.

   b) The platform knows or acts with reckless disregard for the fact that the content meets the requirements prescribed by this bill.

   c) Does not contain a disclosure stating that the media has been manipulated.

2) Requires platforms to develop and implement procedures for identifying and labeling content if the content is reported, posted outside of the time period described in (1) or appears within an advertisement or election communication not subject to (1), and the platform knows or acts with reckless disregard for that fact that the content meets the requirements of the bill. Requires platforms, upon determining the content meets the requirements of labelling and during a specified time period, to label the post, but no later than 72 hours after a report is made.

3) Requires platforms to provide a way for Californians to report content that was not properly blocked or labeled on the platform. Allows a candidate, elected official, or elections official who reported content to the platform but does not receive a response in 36 hours or disagrees with the response – as well as the Attorney General (AG), a district attorney, or a city attorney – to seek injunctive or other equitable relief against a platform to compel compliance with this bill.

4) Provides this bill does not apply to a regularly-published online periodical or broadcast that publishes materially deceptive content that contains a clear disclosure that the content is not an accurate representation of reality or when specified conditions are met. The bill does not apply to materially deceptive content that constitutes as satire or parody.

5) Defines the following terms for the purposes of this bill:

   a) "Deepfake" to mean audio or visual media that is digitally created or modified such that it would falsely appear to a reasonable person to be an authentic record of the actual speech or conduct of the individual depicted in the media;

   b) "Materially deceptive content" to mean audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and the output of chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content depicted in the media; and

   c) "Large online platform" to mean a public-facing internet website, web application, digital application, video sharing platform, advertising network, or search engine that had at least one million California users in the preceding 12 months.

6) Addresses chaptering issues between this bill and AB 2839.

Background

Artificial Intelligence (AI) and Elections. On June 4, 2024, the Senate Committee on Elections and Constitutional Amendments and the Assembly Committee on Elections held a joint information hearing focusing on AI and elections.

The purpose of the hearing was to inform and assist the Legislature in making informed decisions on legislation related to AI-generated and altered content. It became evident that the ease with which people can create and spread mis- and disinformation creates a world where many people may have trouble determining what is fact and what is fiction. The development of increasingly advanced AI tools has made once time-consuming activities much easier to complete, while also enabling the completion of tasks that are otherwise too complex for humans to tackle alone.

State Action. In 2018, the Legislature approved and Governor Brown signed AB 3075 (Berman, Chapter 241, Statutes of 2018) to establish the Office of Elections Cybersecurity (OEC) in the Secretary of State's (SOS) office. The OEC has two primary missions. First, it is responsible for coordinating efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation.

In 2019, the Legislature approved and Governor Newsom signed AB 730 (Berman, Chapter 493, Statutes of 2019). AB 730 sought to address concerns that deepfake technology could be used to spread misinformation in political campaigns. Legislative analyses of AB 730 described "deepfake technology" as software capable of producing a realistic looking video of someone saying or doing something they did not actually say or do.

AB 730 prohibits anyone from distributing deceptive audio or visual media with actual malice and the intent to injure a candidate's reputation or to deceive a voter, unless the media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, but also to any intentional manipulation of audio or visual images where a reasonable person would be misled into believing it was authentic. Notably, AB 730 focused on materially deceptive representations

of candidates, and not on deceptive media of other aspects of the electoral process. AB 730 included a January 1, 2023 sunset date, but in 2022, the Legislature approved AB 972 (Berman, Chapter 745, Statutes of 2022) to extend the sunset date to January 1, 2027.

Comments

1) *According to the Author:* "AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in technology make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy."

2) *First Amendment Considerations.* The First Amendment to the United States (US) Constitution provides in relevant part "Congress shall make no law…abridging the freedom of speech…" Similarly, Section 2 of Article I of the California Constitution provides in relevant part "Every person may freely speak, write, and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press."

   This bill seeks to regulate the distribution by online platforms of media containing intentionally manipulated images, audio, or video related to candidates, elections officials, elected officials, and election materials and equipment under certain circumstances. A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California Constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995, 514 US 334).

   This bill targets deceptive content that could undermine the public's trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found the protection of the integrity of elections is

an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds would likely hinge on whether the court finds this bill's provisions to be narrowly tailored.

Related/Prior Legislation

AB 2355 (W. Carrillo, 2024) requires a campaign committee that creates, originally publishes, or originally distributes a political advertisement to include a disclosure stating that the audio, image, or video was generated or substantially altered using AI.

AB 2839 (Pellerin, 2024) prohibits the distribution of campaign advertisements and other election communications that contain media that has been digitally altered in a deceptive way.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee:

- The Department of Justice (DOJ) indicates that it would incur costs of $911,000 in 2024-25, $1.4 million each in 2025-26 and 2026-27, $1.2 million in 2027-28, and $1 million annually thereafter, to implement the provisions of the bill (General Fund).

- By authorizing a claim by specified parties against a large online platform for failing to block or label specified content, this bill could result in an increased number of civil actions. Consequently, the bill could result in potentially significant cost pressures to the courts; the magnitude is unknown (Trial Court Trust Fund (TCTF)). The specific number of new actions that could be filed under the bill also is unknown; however, it generally costs about $1,000 to operate a courtroom for one hour. Courts are not funded on the basis of workload, and increased pressure on TCTF may create a need for increased funding for courts from the General Fund. The enacted 2024-25 budget includes $37 million in ongoing support from the General Fund to continue to backfill TCTF for revenue declines.

SUPPORT: (Verified 8/26/24)

California Initiative for Technology & Democracy (source)
American Federation of State, County and Municipal Employees
Bay Rising

California Environmental Voters
California Voter Foundation
Center for Countering Digital Hate
Chinese Progressive Association
Disability Rights California
Hmong Innovating Politics
League of Women Voters in California
MOVE the Valley
NextGen California
Partnership for the Advancement of New Americans
SEIU California
TechEquity Action
Youth Power Project

OPPOSITION: (Verified 8/26/24)

ACLU California Action
California Chamber of Commerce
Computer and Communications Industry
Electronic Frontier Foundation
First Amendment Coalition
NetChoice
Oakland Privacy
Software and Information Industry Association
TECHNET

ASSEMBLY FLOOR: 56-1, 5/22/24
AYES: Addis, Aguiar-Curry, Alvarez, Arambula, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Juan Carrillo, Wendy Carrillo, Connolly, Mike Fong, Gabriel, Garcia, Gipson, Grayson, Haney, Hart, Irwin, Jackson, Jones-Sawyer, Kalra, Lee, Low, Lowenthal, Maienschein, McCarty, McKinnor, Muratsuchi, Stephanie Nguyen, Ortega, Pacheco, Papan, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Rendon, Reyes, Rodriguez, Blanca Rubio, Santiago, Schiavo, Soria, Ting, Valencia, Ward, Weber, Wicks, Wilson, Wood, Zbur, Robert Rivas
NOES: Dixon

NO VOTE RECORDED: Alanis, Calderon, Cervantes, Chen, Megan Dahle, Davies, Essayli, Flora, Vince Fong, Friedman, Gallagher, Holden, Hoover, Lackey, Mathis, Jim Patterson, Joe Patterson, Luz Rivas, Sanchez, Ta, Villapudua, Waldron, Wallis

Prepared by: Scott Matsumoto / E. & C.A. / (916) 651-4106
8/26/24 17:01:21

****** END ******

EXHIBIT 13

CONCURRENCE IN SENATE AMENDMENTS
AB 2655 (Berman and Pellerin)
As Amended August 23, 2024
Majority vote

SUMMARY

Requires large online platforms, as defined, to remove materially deceptive and digitally modified or created content related to elections, or to label that content, during specified periods before and after an election, if the content is reported to the platform, as specified.

Senate Amendments

1) Provide that a large online platform is required to remove or label content only if that content is first reported to the platform by a California resident as being content that is covered by the provisions of this bill. Require the platform to remove or label the content no later than 72 hours after it is reported.

2) Limit the bill's applicability to content related to elections in California, and to candidates for President and Vice President, statewide office, Board of Equalization, state Legislature, and United States (US) House of Representatives.

3) Reduce the period of time during which materially deceptive content must be labeled such that the period begins six months before an election in California, instead of beginning one year before an election as was provided in the Assembly-approved version of this bill.

4) Specify that the bill does not apply to a broadcasting station in either of the following circumstances:

   a) When it distributes deceptively-altered media as part of its news coverage, as specified, if the media includes a clear acknowledgement that it is not accurately representative.

   b) When it is paid to broadcast materially deceptive content if federal law requires the station to air the advertisement or if the station has its own prohibition and disclaimer requirements that are generally consistent with the requirements of this bill, as specified.

5) Delete provisions of the bill that would have allowed a court to award reasonable attorney's fees and costs to a prevailing plaintiff party in an action brought under this bill.

6) Delete a provision of the bill that would have required a platform to maintain a copy of any content that it blocks or labels under this bill for at least five years.

7) Delete provisions of the bill that would have made it applicable to deceptive and digitally modified or created content related to redistricting.

8) Recast various provisions of the bill to improve clarity, and make other clarifying, technical, and conforming changes.

9) Add double-jointing language to avoid chaptering problems with AB 2839 (Pellerin) of the current legislative session.

COMMENTS

The use of false and deceptive information in campaigns to influence election outcomes is not a new phenomenon. Laws aimed at curbing such practices and preserving the integrity of elections have a long history in California. In 1850, the First Session of the California State Legislature created penalties for election misconduct, including for "deceiving [an elector] and causing him to vote for a different person for any office than such elector desired or intended to vote for" (Chapter 38, Statutes of 1850).

Advancements in technology have made it increasingly simple to produce false and misleading media that closely resembles authentic content. Moreover, platforms like social media have facilitated the rapid dissemination of deceptive media to large audiences at minimal cost. Given these developments, the potential threat posed by manipulated media to future elections' integrity may be more significant than in the past.

Past legislative efforts have addressed concerns about manipulated media's use to deceive voters during elections. Those laws, however, are limited, and are designed primarily to target the harms to *candidates* that may result from the distribution of manipulated media of those candidates. In contrast, this bill aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. Additionally, this bill targets media that portrays elections materials and equipment in materially deceptive ways. The author and supporters of this bill believe that these provisions will safeguard voters against deceitful media that could undermine trust in the electoral process.

The Legislature is considering a number of bills this year that seek to address deceptive and digitally altered elections-related content in an effort to protect the integrity of elections in California. While other legislation related to this topic applies broadly to the distribution of such content through various mediums, this bill specifically targets the distribution of deceptive content through online platforms, including social media. Recognizing that those online platforms can facilitate the rapid spread of deceptive content, this bill seeks to minimize that potential by obligating large online platforms to remove or label offending content.

In recognition that the regulation of the distribution of content can create free speech concerns, this bill contains various provisions that tailor the content to which it applies, such that it targets content that has the highest likelihood of deceiving voters and undermining electoral integrity. While that tailoring does limit the content that online platforms would be required to remove or label, it also adds additional factors that platforms must consider in order to identify content that is required to be removed or labeled under this bill.

Along with other limitations, this bill applies only to content that 1) is distributed during specified time periods around elections and election processes, 2) includes media relating to elections or the electoral process in specified ways, 3) that was intentionally manipulated digitally to be materially deceptive, and 4) that is not satire or parody. Each of these limitations adds additional factors that online platforms would need to consider when determining whether a specific communication must be removed or labeled by this bill. Given the number of elections and candidates in California at any given time, making the determinations at scale about which content must be removed or labeled likely will be considerably more challenging than making those determinations on a case-by-case basis in a court of law. Senate amendments, however, eliminated the requirements for platforms to proactively remove or label such content, and

instead impose an obligation on platforms to act only after a report has been made. Those amendments likely will reduce the burden that this bill creates on platforms to some degree.

A question could be raised about whether this bill is consistent with the right to freedom of speech that is guaranteed by the US and California constitutions. The US Supreme Court has ruled that even false statements are protected by the First Amendment (*United States v. Alvarez* (2012), 567 U.S. 709). When a law burdens core political speech, the restrictions on speech generally must be "narrowly tailored to serve an overriding state interest," *McIntyre v. Ohio Elections Commission* (1995), 514 US 334.

This bill targets deceptive content that could undermine trust in elections, prevent voters from voting, and distort the electoral process. The US Supreme Court generally has found that the protection of the integrity of elections is an overriding (or compelling) government interest (*Id.* at 349; *Burson v. Freeman* (1992) 504 U.S. 191, 199). A challenge of this bill on First Amendment grounds, then, likely would hinge on whether the court found this bill's provisions to be narrowly tailored. This bill includes provisions to limit its scope to communications posing the greatest threat to election integrity in an effort to tailor its provisions. Whether these limitations adequately protect this bill from a potential constitutional challenge is unclear. However, while these limitations may help protect the bill against a constitutional challenge, they may also make it harder for the bill to achieve its aims of limiting the spread of materially deceptive communications that have the potential to undermine election integrity.

The Senate amendments eliminate the requirement for platforms to proactively block or label deceptive content, and instead require platforms to address deceptive content only upon receiving reports from users about that content. The Senate amendments additionally make various changes in response to opposition concerns including narrowing the bill's applicability to broadcast stations and limiting the types of elections and candidates to which the bill applies, among other changes.

Please see the policy committee analysis for a full discussion of this bill.

According to the Author
"AB 2655 will ensure that online platforms restrict the spread of election-related deceptive deepfakes meant to prevent voters from voting or to deceive them based on fraudulent content. Deepfakes are a powerful and dangerous tool in the arsenal of those that want to wage disinformation campaigns, and they have the potential to wreak havoc on our democracy by attributing speech and conduct to a person that is false or that never happened. Advances in AI make it easy for practically anyone to generate this deceptive content, making it that much more important that we identify and restrict its spread before it has the chance to deceive voters and undermine our democracy."

Arguments in Support
The sponsor of this bill, the California Initiative for Technology & Democracy, writes in support, "Those trying to influence campaigns – conspiracy theorists, foreign states, online trolls, and candidates themselves – are already creating and distributing election-threatening deepfake images, audio, and video content in the US and around the world… AB 2655 strikes the right balance by seeking to ban, for a strictly limited time before and after elections, the online spread of the worst deepfakes and disinformation maliciously intended to prevent voters from voting or getting them to vote erroneously based on fraudulent content. The bill also requires that other fake online content related to elections and elections processes…which is also designed to

undermine election procedures and democratic institutions, must be labeled as fake, again just for a limited time. The bill only applies to the largest online platforms with the greatest reach of potential election disinformation, and we believe it is fully implementable today based on tools these companies already possess… AB 2655's approach is narrowly tailored and does not extend the law to hot button controversies or inflammatory claims…It simply stops the use of obviously, demonstrably untrue and provably false content meant to impermissibly influence our elections at peak election times. It is therefore respectful of the protections of the First Amendment and avoids concerns based on Section 230 of the Communications Decency Act."

Arguments in Opposition
A coalition of business and technology industry associations writes in opposition, "AB 2655 appears to be based on the false assumption that online platforms definitively know whether any particular piece of content has been manipulated in such a way that is defined under the bill. While digital services may employ tools to identify and detect these materials with some degree of certainty, it is an evolving and imperfect science in its current form. AB 2655 also presumes that online platforms are an appropriate arbiter of deciding what constitutes accurate election information. However, most digital services are not equipped with the tools or expertise to make such judgments. Because covered platforms are not privy to the intent and context behind each piece of content, they may inadvertently over-block or over-label material. This could lead to user frustration and the suppression of political speech. Political speech is fundamental to the First Amendment's purpose. Therefore, AB 2655 raises concerns about how its provisions could have a chilling effect on online speech and whether it can withstand constitutional scrutiny."

FISCAL COMMENTS

According to the Senate Appropriations Committee:

1) The Department of Justice (DOJ) indicates that it would incur costs of $911,000 in 2024-25, $1.4 million each in 2025-26 and 2026-27, $1.2 million in 2027-28, and $1 million annually thereafter, to implement the provisions of the bill (General Fund).

2) By authorizing a claim by specified parties against a large online platform for failing to block or label specified content, this bill could result in an increased number of civil actions. Consequently, the bill could result in potentially significant cost pressures to the courts; the magnitude is unknown (Trial Court Trust Fund (TCTF)). The specific number of new actions that could be filed under the bill also is unknown; however, it generally costs about $1,000 to operate a courtroom for one hour. Courts are not funded on the basis of workload, and increased pressure on TCTF may create a need for increased funding for courts from the General Fund. The enacted 2024-25 budget includes $37 million in ongoing support from the General Fund to continue to backfill TCTF for revenue declines.

VOTES:

ASM ELECTIONS: 6-1-1
YES: Pellerin, Bennett, Berman, Cervantes, Low, Weber
NO: Essayli
ABS, ABST OR NV: Lackey

ASM JUDICIARY: 9-0-3
YES: Kalra, Bauer-Kahan, Bryan, Connolly, Haney, Maienschein, McKinnor, Pacheco, Reyes

ABS, ABST OR NV: Dixon, Sanchez, Waldron

ASM APPROPRIATIONS: 11-1-3
YES: Wicks, Arambula, Bryan, Calderon, Wendy Carrillo, Mike Fong, Grayson, Haney, Hart, Pellerin, Villapudua
NO: Dixon
ABS, ABST OR NV: Sanchez, Jim Patterson, Ta

ASSEMBLY FLOOR: 56-1-23
YES: Addis, Aguiar-Curry, Alvarez, Arambula, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Juan Carrillo, Wendy Carrillo, Connolly, Mike Fong, Gabriel, Garcia, Gipson, Grayson, Haney, Hart, Irwin, Jackson, Jones-Sawyer, Kalra, Lee, Low, Lowenthal, Maienschein, McCarty, McKinnor, Muratsuchi, Stephanie Nguyen, Ortega, Pacheco, Papan, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Rendon, Reyes, Rodriguez, Blanca Rubio, Santiago, Schiavo, Soria, Ting, Valencia, Ward, Weber, Wicks, Wilson, Wood, Zbur, Robert Rivas
NO: Dixon
ABS, ABST OR NV: Alanis, Calderon, Cervantes, Chen, Megan Dahle, Davies, Essayli, Flora, Vince Fong, Friedman, Gallagher, Holden, Hoover, Lackey, Mathis, Jim Patterson, Joe Patterson, Luz Rivas, Sanchez, Ta, Villapudua, Waldron, Wallis

SENATE FLOOR: 31-9-0
YES: Allen, Archuleta, Ashby, Atkins, Becker, Blakespear, Bradford, Caballero, Cortese, Dodd, Durazo, Eggman, Glazer, Gonzalez, Hurtado, Laird, Limón, McGuire, Menjivar, Min, Newman, Padilla, Portantino, Roth, Rubio, Skinner, Smallwood-Cuevas, Stern, Umberg, Wahab, Wiener
NO: Alvarado-Gil, Dahle, Grove, Jones, Nguyen, Niello, Ochoa Bogh, Seyarto, Wilk

UPDATED

VERSION: August 23, 2024

CONSULTANT: Ethan Jones / ELECTIONS / (916) 319-2094 FN: 0004820

EXHIBIT 14

Settings

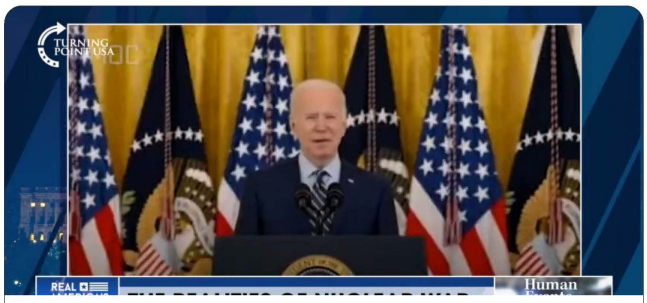
Post

Jack Poso
@JackPosobiec

"The recommended way forward will be to invoke the Selective Service Act, as is my authority as president"

"The first to be called will be men and women who's 20th birthday falls during calendar year 2023"

A sneak preview of things to come



0:06 / 3:15

From **The Post Millennial**

Readers added context they thought people might want to know

This presenter retweeted an AI video without including the written warning that this has been created by AI like the original creator did.

twitter.com/tpostmillennia...

Context is written by people who use X, and appears when rated helpful by others. Find out more.

9:48 AM · Feb 27, 2023 · **7.1M** Views

4K 4.8K 10K 947

Read 4K replies

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

Retry

Terms of Service Privacy Policy Cookie Policy
Accessibility Ads info More ··· © 2025 X Corp.

Don't miss what's happening
People on X are the first to know.

Log in Sign up

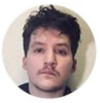
Exhibit 14
Page 149

EXHIBIT 15

TECH

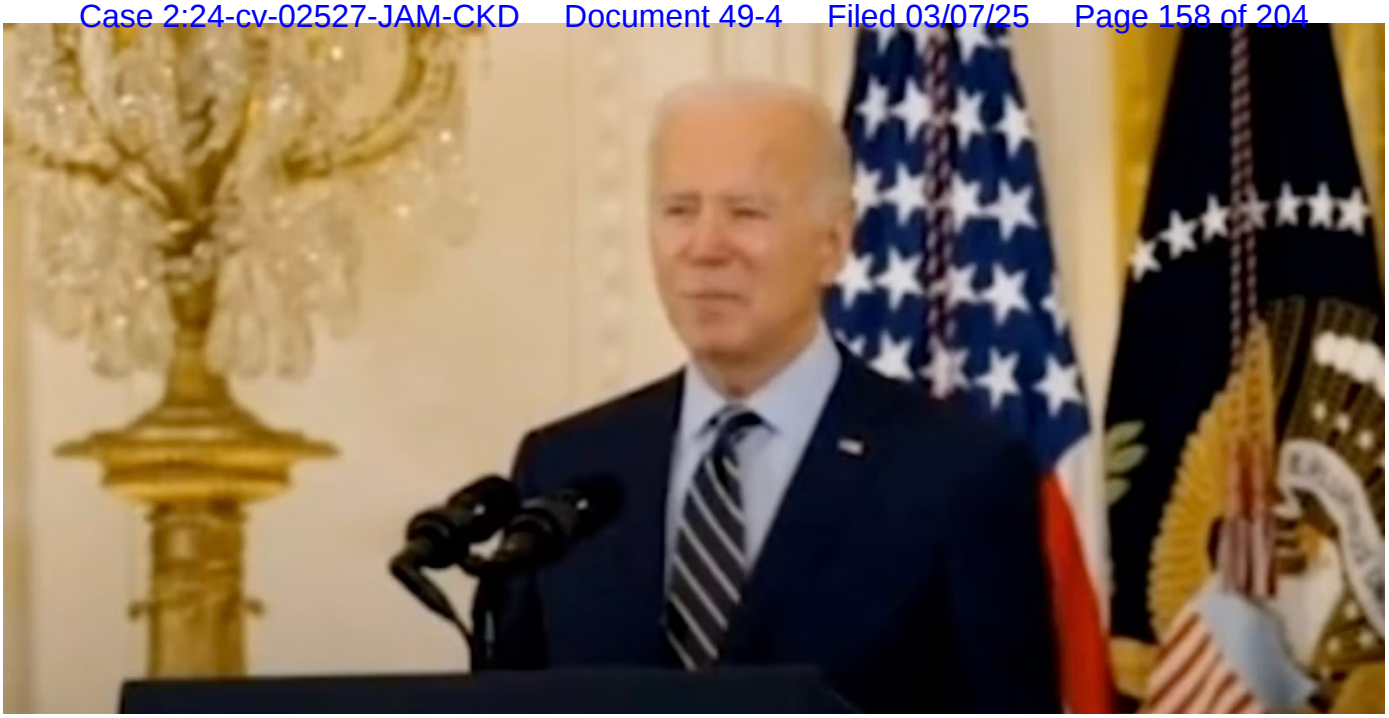
‘Legitimate use of deepfakes’: AI-generated video of Biden declaring World War 3, bringing back draft splits experts

‘A sneak preview of things to come.’



Mikael Thalen

Posted on March 2 2023 1:09 pm CST



The Post Millennial Live/Rumble

Right-wing commentator Jack Posobiec aired a deepfake video of President Joe Biden this week announcing the return of the military draft and the beginning of a third world war.

Experts are split on whether it was a dangerous misuse of the technology or an actual example of how the medium can be handled responsibly.

The video, which Posobiec predicted was a “sneak preview” of things to come, was shared with his more than 2 million followers on Twitter.

The footage features a chyron that references “the realities of nuclear war” and depicts Biden invoking the Selective Service Act due to growing tensions with Russia and China.

“The illegal Russian offensive has been swift, callous, and brutal. It’s barbaric,” the AI-generated Biden states. “Putin’s illegal occupation of Kyiv and the impending Chinese blockade of Taiwan has created a two-front national security crisis that requires more troops than the volunteer military can supply.”

Once the clip finishes, Posobiec appears on screen to offer commentary on the AI-generated scenario.

“What we just played for you was a sneak preview, coming attractions, a glimpse into the world beyond,” he says. “Now that was an AI, I don’t want to say a recreation but maybe a pre-creation… a pre-creation of President Biden designed and scripted by our producers here for the show of what could happen if President Biden were to declare and activate the Selective Service Act and begin drafting 20-year-olds here in the United States.”

The segment proved controversial online, with some referring to the display as “nauseatingly irresponsible.”

“Creating something like this is so nauseatingly irresponsible, in such bad faith, and such a waste of resources I can only be completely unsurprised,” one critic tweeted.

Concerns were also raised over the ability of people watching to differentiate between legitimate and manipulated media.

Despite both the tweet and Posobiec stating that the video was in fact created with AI, one of the first commenters on the video nonetheless asked if what they were seeing was real.

“Is this legit, or some sort of AI deepfake clips?” one user asked.

https://twitter.com/SirWestmoore/status/1630388057684811776?s=20

Speaking with the Daily Dot, author and generative AI expert Nina Schick argued that the advancement of AI-related technologies will lead to further degradation of trust in content seen online even when it is specified as manipulated.

“We’re going to see a lot more AI-generated content that will be in the context where it is marked as being AI-generated but people are still fooled,” she said.

Twitter initially responded to the video by placing a fact-check notice on the tweet. The notice was removed soon after though, likely given that the footage clearly noted that it had been created by AI.

“They took the fact-check off of this tweet and BlueAnon is melting down saying I am now attempting to create a domestic insurrection,” Posobiec tweeted. “Stay mad, freaks!”

The Daily Dot reached out to Posobiec over the contact form on his media website Human Events but did not receive a reply by press time.

On the other hand, Sam Gregory, a deepfake expert and the program director at the human rights organization WITNESS, said that the video was an example of a “legitimate use of

deepfakes."

"The video is a visualization of a hypothetical or a potential future to further a discussion, and importantly it's contextualized as such," Gregory told the Daily Dot. "We've already seen AI-generated imagery used to present potential climate futures, offer unexpected satirical voices of politicians and 'deepfake it till they do it', and offer perspectives on current events and realities from people who have died with resurrection deepfakes."

Gregory also said he appreciated that Posobiec didn't use the video to warn about the dangers of deepfakes, which he described as "an over-used technique" that "seems to contribute to undermining trust in real media," but to focus on a political hypothetical.

"As we approach deepfakes and synthetic media regulation and norms it's important we protect expressive speech, political speech, and satire," he added. "However, I do think that it's key that we also think how—particularly now when people are not clear what can and can't be faked—that we also emphasize visible disclosure and labeling in places like TV and web use of 'news-like' deepfakes."

While feelings towards Posobiec's video fall largely along political lines across social media, experts continue to argue that such issues are much more complex.

Synthetic media expert Henry Ajder likewise noted that although the video clearly labels itself as AI-generated, even honest deepfakes can produce the same issues as those made deceptively.

"This deepfake is clearly designed to grab viewers' attention before being clearly disclosed as fake, but if taken out of context in our fractious information ecosystem, the audience response could be very different," Ajder said in a statement to the Daily Dot. "In this respect,

artistic or well-meaning deepfake content can still fall victim to the crude forms of media manipulation that are much more prominent online. Creators need to consider not just how they intend generative content to be received, but how it could be misrepresented when released 'into the wild.'"

Such content will undoubtedly become exponentially more commonplace as the barrier to entry continues to drop for AI-related technologies. It's genuinely unclear whether the public is truly ready.

MORE IN TECH

Sam Bankman-Fried is following his leaked image rehab game plan to a T

Prominent detransitioner ‘Maia Poet’ accused of familial ties to vocal anti-trans advocacy group

Elon Musk’s government email leaked—and people are already bombarding it

The deep state is trying to kill RFK Jr.(‘s character)

Share this article

TAGS DEEPFAKES JACK POSOBIEC JOE BIDEN WAR

First published: Mar 2, 2023, 1:09 pm CST

Mikael Thalen

Mikael Thalen is a tech and security reporter covering social media, data breaches, hackers, and more.

Exhibit 15
Page 161

EXHIBIT 16

Fake AI images of Putin, Trump being arrested spread online

Politics Mar 23, 2023 3:35 PM EST

NEW YORK (AP) — **Former President Donald Trump** getting gang-tackled by riot-gear-clad New York City police officers. Russian President Vladimir Putin in prison grays behind the bars of a dimly lit concrete cell.

The highly detailed, sensational images have inundated Twitter and other platforms in recent days, amid news that Trump faces possible criminal charges and the International Criminal Court has issued an arrest warrant for Putin.

But neither visual is remotely real. The images — and scores of variations littering social media — were produced using increasingly sophisticated and widely accessible image generators powered by artificial intelligence.

Misinformation experts warn the images are harbingers of a new reality: waves of fake photos and videos flooding social media after major news events and further muddying fact and fiction at crucial times for society.

“It does add noise during crisis events. It also increases the cynicism level,” said Jevin West, a professor at the University of Washington in Seattle who focuses on the spread of misinformation. “You start to lose trust in the system and the information that you are getting.”

While the ability to manipulate photos and create fake images isn’t new, AI image generator tools by Midjourney, DALL-E and others are easier to use. They can quickly generate realistic images — complete with detailed backgrounds — on a mass scale with little more than a simple text prompt from users.

WATCH: Security expert warns of AI tools’ potential threat to democracy

Some of the recent images have been driven by **this month’s release** of a new version of Midjourney’s text-to-image synthesis model, which can, among other things, now produce convincing images mimicking the style of news agency photos.

In one widely-circulating Twitter thread, Eliot Higgins, founder of Bellingcat, a Netherlands-based investigative journalism collective, used the latest version of the tool to conjure up **scores of dramatic images** of Trump’s fictional arrest.

The visuals, which have been shared and liked tens of thousands of times, showed a crowd of uniformed officers grabbing the Republican billionaire and violently pulling him down onto the pavement.

Higgins, who was also behind a **set of images** of Putin being arrested, put on trial and then imprisoned, says he posted the images with no ill intent. He even stated clearly in his Twitter thread that the images were AI-generated.

Still, the images were enough to get him locked out of the Midjourney server, according to Higgins. The San Francisco-based independent research lab didn’t respond to emails seeking comment.

“The Trump arrest image was really just casually showing both how good and bad Midjourney was at rendering real scenes,” Higgins wrote in an email. “The images started to form a sort of narrative as I plugged in prompts to Midjourney, so I strung them along into a

narrative, and decided to finish off the story."

He pointed out the images are far from perfect: in some, Trump is seen, oddly, wearing a police utility belt. In others, faces and hands are clearly distorted.

But it's not enough that users like Higgins clearly state in their posts that the images are AI-generated and solely for entertainment, says Shirin Anlen, media technologist at Witness, a New York-based human rights organization that focuses on visual evidence.

READ MORE: How AI turns text into images

Too often, the visuals are quickly reshared by others without that crucial context, she said. Indeed, an Instagram post sharing some of Higgins' images of Trump as if they were genuine garnered more than 79,000 likes.

"You're just seeing an image, and once you see something, you cannot unsee it," Anlen said.

In another recent example, social media users shared a synthetic image supposedly capturing Putin kneeling and kissing the hand of Chinese leader Xi Jinping. The image, which circulated as the Russian president welcomed Xi to the Kremlin this week, quickly became a crude meme.

It's not clear who created created the image or what tool they used, but some clues gave the forgery away. The heads and shoes of the two leaders were slightly distorted, for example, and the room's interior didn't match the room where the actual meeting took place.

With synthetic images becoming increasingly difficult to discern from the real thing, the best way to combat visual misinformation is better public awareness and education, experts say.

"It's just becoming so easy and it's so cheap to make these images that we should do whatever we can to make the public aware of how good this technology has gotten," West said.

Higgins suggests social media companies could focus on developing technology to detect AI-generated images and integrate that into their platforms.

Twitter has a policy banning "synthetic, manipulated, or out-of-context media" with the potential to deceive or harm. Annotations from Community Notes, Twitter's crowd-sourced fact checking project, were attached to some tweets to include the context that the Trump images were AI-generated.

When reached for comment Thursday, the company emailed back only an automated response.

Meta, the parent company of Facebook and Instagram, declined to comment. Some of the fabricated Trump images were labeled as either "false" or "missing context" through its third-party fact-checking program, of which the AP is a participant.

Arthur Holland Michel, a fellow at the Carnegie Council for Ethics in International Affairs in New York who is focused on emerging technologies, said he worries the world isn't ready for the impending deluge.

He wonders how deepfakes involving ordinary people — harmful fake pictures of an ex-partner or a colleague, for example — will be regulated.

"From a policy perspective, I'm not sure we're prepared to deal with this scale of disinformation at every level of society," Michel wrote in

an email. “My sense is that it’s going to take an as-yet-unimagined technical breakthrough to definitively put a stop to this.”

Associated Press reporter David Klepper in Washington contributed to this story.

By — **Arijeta Lajka, Associated Press**

By — **Philip Marcelo, Associated Press**

Why ‘deepfake’ videos are becoming more difficult to detect

Science Jun 12

EXHIBIT 17

POLITICO

ELECTIONS

DeSantis PAC uses AI-generated Trump voice in ad attacking ex-president

The spot illustrates the new frontiers in political advertising.

A person familiar with the ad confirmed former President Donald Trump's voice was AI generated. | Charlie Neibergall/AP Photo

By ALEX ISENSTADT
07/17/2023 06:21 PM EDT

A pro-Ron DeSantis super PAC uses an Artificial Intelligence version of Donald Trump's voice in a new television ad attacking the former president.

The ad, from Never Back Down, charges Trump with attacking Iowa Gov. Kim Reynolds as part of a larger pattern of disrespect he has shown to the first caucus state.

But the audio that the spot uses is not actually from Trump. A person familiar with the ad confirmed Trump's voice was AI generated. Its content appears to be based off of a post that Trump made on his social media site Truth Social last week. The person said it will run statewide in Iowa tomorrow and that the ad buy was at least $1 million — a massive sum though one doable for the well-heeled super PAC. It will also be running via text message and on digital platforms.

Political ads have used impersonation before, and the Trump-generated voice in the Never Back Down ad does not sound entirely natural. Still, the spot highlights what could be the next frontier of campaign advertising: The use of AI-generated content to produce increasingly difficult to identify, so-called deepfakes.

"The blatant use of AI to fabricate President Trump's voice is a desperate attempt by Always Back Down and Jeff Roe to deceive the American public because they know DeSanctimonious' campaign is on life support," said Trump campaign senior adviser Chris LaCivita, referring to a top official with the pro-DeSantis super PAC. "After losing big donors and slashing their staff, they have now outsourced their work to AI just like they would like to outsource American jobs to China."

Never Back Down had previously used AI to superimpose a fighter jet into a pro-DeSantis ad.

FILED UNDER: ADVERTISEMENTS, RON DESANTIS, KIM REYNOLDS,

EXHIBIT 18

New Hampshire
Department of Justice
Office of the Attorney General

OPEN MENU

Press Release

For Immediate Release
Date: May 23, 2024

Contact
Michael S. Garrity, Director of Communications
(603) 931-9375 | michael.s.garrity@doj.nh.gov

Brendan O'Donnell, Assistant Attorney General, Election Law Unit

Steven Kramer Charged with Voter Suppression Over AI-Generated President Biden Robocalls

Concord, NH – Attorney General John M. Formella announces that today, Steven Kramer, age 54, of New Orleans, LA, has been indicted on charges of felony voter suppression and misdemeanor impersonation of a candidate.

On January 22, 2024, this Office announced that it was opening an investigation into reports of thousands of New Hampshire residents receiving a robocall message asking them to "save [their] vote for the November election" and stating "[y]our vote makes a difference in November, not this Tuesday." The voice in the recorded message appeared to have been artificially generated to sound like the voice of President Biden. The message additionally appeared to have been "spoofed" to falsely show that it had been sent by the treasurer of a political committee that had been supporting the New Hampshire Democratic Presidential Primary write-in efforts for President Biden.

Following an investigation, Mr. Kramer has been charged with 13 felony counts of voter suppression, contrary to RSA 659:40, III, and 13 misdemeanor counts of impersonation of a candidate, contrary to RSA 666:7-a. The charges are spread across four counties based on the residence of thirteen New Hampshire residents who received the Biden Robocalls: Rockingham County (five counts of violating each statute); Belknap County (three counts); Grafton County (three counts); Merrimack County (two counts).

"New Hampshire remains committed to ensuring that our elections remain free from unlawful interference and our investigation into this matter remains ongoing. The Federal Communications Commission will separately be announcing an enforcement action against Mr. Kramer based on violations of federal law. I am pleased to see that our federal partners are similarly committed to protecting consumers and voters from harmful robocalls and voter suppression," said Attorney General Formella. "I hope that our respective enforcement actions send a strong deterrent signal to anyone who might consider interfering with elections, whether through the use of artificial intelligence or otherwise."

RSA 659:40, III provides: "No person shall engage in voter suppression by knowingly attempting to prevent or deter another person from voting or registering to vote based on fraudulent, deceptive, misleading, or spurious grounds or information." The RSA 659:40, III charges allege that Mr. Kramer violated the statute by sending or causing to be sent a pre-recorded phone message that disguised the source of the call, deceptively using an artificially created voice of a candidate, or providing misleading information in an attempt to deter thirteen identified voters from voting in the January 23, 2024 Presidential Primary Election.

RSA 666:7-a provides: "Any person who places a telephone call during which the person falsely represents himself or herself as a candidate for office shall be guilty of a misdemeanor." The RSA 666:7-a charges allege that Mr. Kramer, by his own conduct or by the conduct of another person for which he is legally accountable, violated the statute by knowingly placing a telephone call to thirteen identified voters during which Mr. Kramer falsely represented himself as a candidate for office.

The charges and allegations against Mr. Kramer are merely accusations, and Mr. Kramer is presumed innocent unless and until proven guilty.

This matter was investigated by Investigator Richard Tracy of the Department of Justice's Election Law Unit. The criminal case is being prosecuted by Assistant Attorneys General Brendan O'Donnell and Matthew Conley, also of the Election Law Unit.

The investigation into the AI-Generated President Biden Robocalls, including other potentially responsible parties, remains active and ongoing.
NOTE: Separate Federal Communications Commission Announcements:

Lingo Telecom Robocall Notice

Steve Kramer Robocall Notice

New Hampshire
Department of Justice
Office of the Attorney General

1 Granite Place South | Concord, NH | 03301
(603) 271-3658

COVID-19 Resources

Exhibit 18
Page 172

NH Government Careers

NH Travel & Tourism

NH Web Portal - NH.gov

ReadyNH.gov

Transparent NH

EXHIBIT 19

FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC PROPOSES $6 MILLION FINE FOR ILLEGAL ROBOCALLS THAT USED BIDEN DEEPFAKE GENERATIVE AI VOICE MESSAGE

Steve Kramer Instigated Illegal Robocall and Spoofing Campaign Telling Voters Not to Vote in 2024 New Hampshire Primary

WASHINGTON, May 23, 2024—The Federal Communications Commission today proposed a substantial fine for apparently illegal robocalls made using deepfake, AI-generated voice cloning technology and caller ID spoofing to spread election misinformation to potential New Hampshire voters prior to the January primary. Steve Kramer faces a $6 million proposed fine for apparent spoofing violations.

Two days before the New Hampshire 2024 presidential primary election, illegally spoofed and malicious robocalls carried a deepfake audio recording of President Biden's cloned voice telling prospective voters not to vote in the upcoming primary. Political consultant Steve Kramer was responsible for the calls and now faces a $6 million proposed fine for perpetrating this illegal robocall campaign on January 21, 2024. The calls apparently violated the Truth in Caller ID Act by maliciously spoofing the number of a prominent local political consultant. The robocalls, made two days prior to the election, used a deepfake of President Biden's voice and encouraged voters to not vote in the primary but rather to "save your vote for the November election." Commission rules prohibit knowingly causing the transmission of inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value. Mr. Kramer's conduct apparently runs afoul of this rule.

"We will act swiftly and decisively to ensure that bad actors cannot use U.S. telecommunications networks to facilitate the misuse of generative AI technology to interfere with elections, defraud consumers, or compromise sensitive data," said **Loyaan A. Egal, Chief of the Enforcement Bureau and chair of the Privacy and Data Protection Task Force**. "We thank our partners at the New Hampshire Attorney General's Office for their help with this investigation."

To transmit the calls, Mr. Kramer had engaged Voice Broadcasting Corp., which used the services of Life Corp. to transmit calls through voice service provider Lingo Telecom. Lingo Telecom transmitted these calls, incorrectly labeling them with the highest level of caller ID attestation, making it less likely that other providers could detect the calls as potentially spoofed. The Commission brought a separate enforcement action today against Lingo Telecom for apparent violations of STIR/SHAKEN for failing to utilize reasonable "Know Your Customer" protocols to verify caller ID information in connection with Mr. Kramer's illegal robocalls.

In February, the FCC's Enforcement Bureau, in coordination with the office of the New Hampshire Attorney General, ordered Lingo to cease-and-desist from carrying the suspicious traffic. The Commission has taken such actions to block active robocall scam campaigns, in addition to imposing financial penalties like those proposed today. These efforts to stop active campaigns have had important impacts, including FCC actions that resulted in a 99% drop in auto

warranty scam robocalls, an 88% month-to-month drop in student loan scam robocalls, and the end to a predatory mortgage robocall campaign targeting homeowners nationwide.

The FCC continues its work in understanding and adjusting to the impacts of AI on robocalling and robotexting. The Commission has made clear that calls made with AI-generated voices are "artificial" under the Telephone Consumer Protection Act (TCPA), confirming that the FCC and state Attorneys General have the needed tools to go after bad actors behind these nefarious robocalls. In addition, the FCC launched a formal proceeding to gather information on the current state of AI use in calling and texting and ask questions about new threats, like robocalls mimicking the voices of those we know. The FCC also co-hosted a workshop with the National Science Foundation that convened stakeholders to discuss AI-related topics including the challenges AI brings to consumer issues like robocalls/robotexts.

The proposed action, formally called a Notice of Apparent Liability for Forfeiture, or NAL, contains only allegations that advise a party on how they have apparently violated the law and may set forth a proposed monetary penalty. The Commission may not impose a greater monetary penalty than the amount proposed in the NAL. Neither the allegations nor the proposed sanctions in the NAL are final Commission actions. Kramer will be given an opportunity to respond and the Commission will consider submissions of evidence and legal arguments before acting further to resolve these matters.

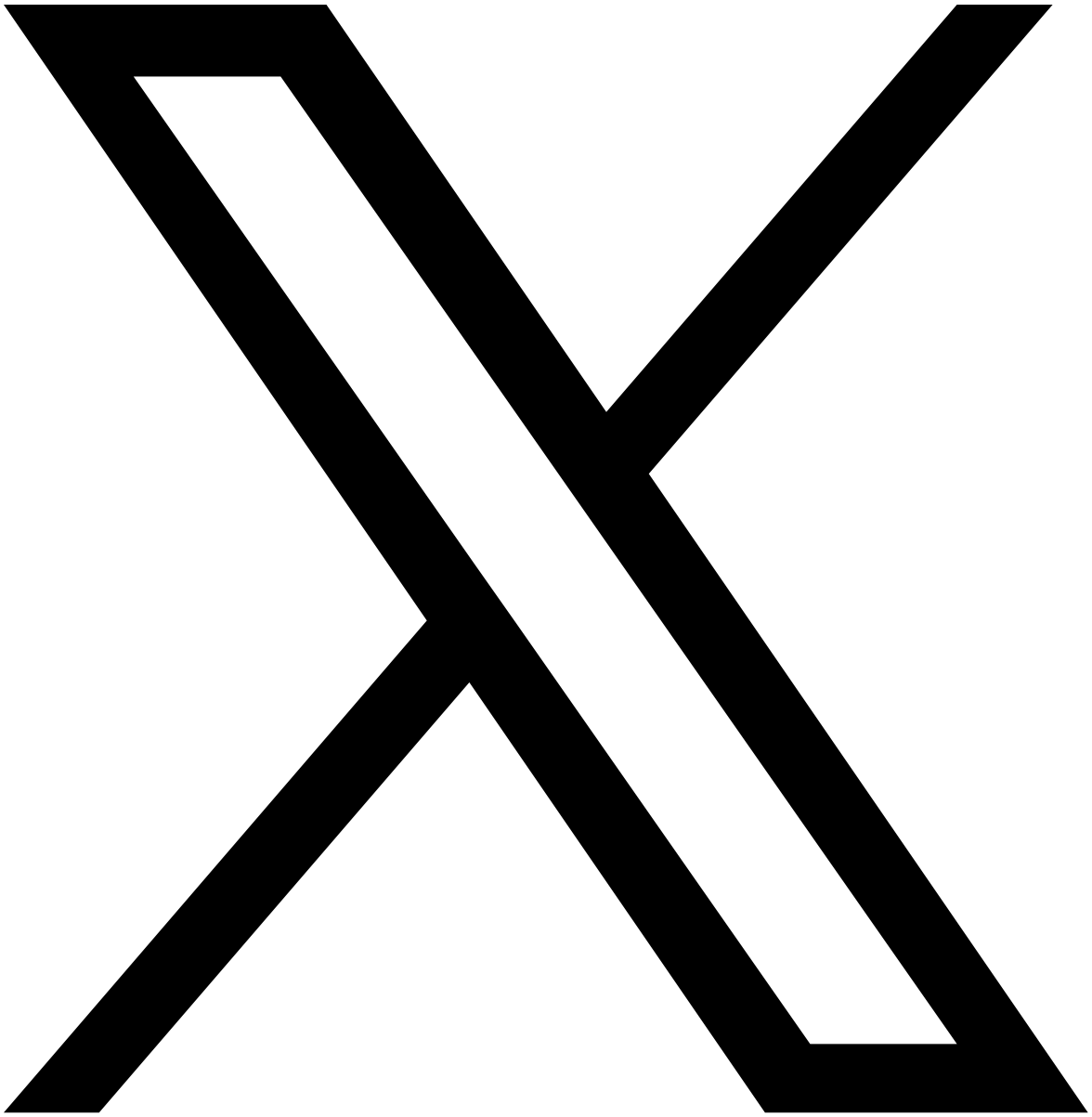
Action by the Commission May 23, 2024 by Notice of Apparent Liability for Forfeiture (FCC 24-59). Chairwoman Rosenworcel, Commissioners Carr, Starks, Simington, and Gomez approving. Chairwoman Rosenworcel, Commissioners Starks and Gomez issuing separate statements.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / www.fcc.gov

EXHIBIT 20

Skip to main content



Help Center (https://help.x.com/en)

Report violations

1. Help Center (https://help.x.com/en)
2. Platform Use Guidelines (https://help.x.com/en/rules-and-policies#platform-use-guidelines)

Report violations

This article provides an overview of how to report potential violations of the X Rules and Terms of Service.

How to report directly from a post, List, or profile

You can report directly from an individual post, List, or profile for certain violations, including: spam, abusive or harmful content, inappropriate ads, self-harm and impersonation. For information about reporting other types of violations, see the **How to report specific types of violations** section below.

How to report individual posts for violations:

Learn how to report posts, Lists, or Direct Messages for violations.

How to report media for violations:

Learn how to report posts for media, and read the X media policy.

How to report profiles for violations:

1. Open the profile you'd like to report.
2. Select the **overflow** icon °°°
3. Select **Report** and then select the type of issue you'd like to report.
4. If you select **They're being abusive or harmful**, we'll ask you to provide additional information about the issue you're reporting. We may also ask you to select additional posts from the account you're reporting so we have better context to evaluate your report.
5. We will include the text of the posts you reported in our follow-up emails and notifications to you. To opt-out of receiving this information, please uncheck the box next to **Updates about this report can show these posts**.
6. Once you've submitted your report, we'll provide recommendations for additional actions you can take to improve your X experience.

How to report specific content in a Moment

How to report a post in a Moment for violations:

1. Navigate to the post within the Moment that you'd like to report.
2. Click or tap the °°° icon.
3. Click or tap **Report post**.
4. Choose the type of issue you'd like to report to us.
5. Once you've submitted your report, we'll provide recommendations for actions you can take to improve your X experience.

How to report Moment for violations:

Depending on what type of violation you're reporting, there are several ways to report a Moment. Below is a list of the types of violations you might see:

- Violation of posting private information (https://help.twitter.com/en/forms/safety-and-sensitive-content/private-information)
- Abuse (https://help.twitter.com/en/forms/safety-and-sensitive-content/abuse)
- Hateful conduct (https://help.twitter.com/en/forms/safety-and-sensitive-content/hateful-conduct)
- Violent threats (https://help.twitter.com/en/forms/safety-and-sensitive-content/violent-threats)
- Self harm (https://help.twitter.com/en/forms/safety-and-sensitive-content/self-harm)

Once you've identified the type of violation you need to report, follow the instructions below.

1. Chose one of the forms listed above.
2. Enter the Moment URL that you would like to report.
3. Provide us with up to 5 posts within the Moment that may be in violation.
4. Once you've submitted your report, we'll provide recommendations for actions you can take to improve your X experience.

How to report a X Space or person in a Space

If you think a Space or someone in a Space violates the X Rules and policies, you can report them. Speakers and listeners can report a Space and any account in a Space.

How to report a Space for violations:

1. While in the Space, tap the overflow icon °°°.
2. Tap **Report this Space**.
3. Select the type of issue you'd like to report to us.
4. Once you've reported the Space, you'll have the option to leave or stay.

How to report an account for violations:

1. While in the Space, tap on the account's profile photo.
2. Tap **Report**.
3. Select the type of issue you'd like to report to us.
4. Once you've reported the account, you'll have the option to leave or stay in the Space.

How to report a product

If you think a product from a merchant on X violates our Shopping Policies, you can report them directly from your X for iOS or Android App.

How to report a product from a Shop Spotlight (https://blog.twitter.com/en_us/topics/product/2021/twitter-shopping--testing-shoppable-profiles-on-twitter) :

1. While on a merchant's profile, find the Shop Spotlight.
2. Select the more icon ••• on the product you wish to report.
3. Select **Report product.**
4. Select **Intellectual property violation** if you're reporting a product for issues with intellectual property rights. (https://help.twitter.com/en/rules-and-policies#intellectual-property) You'll need to include the product ID. (https://help.twitter.com/en/using-twitter/tweet-and-moment-url#productid) You can also submit an intellectual property violation directly here (https://help.twitter.com/en/forms/ipi).

   Select **Other violation** if you're reporting a product for a different reason.

How to report a product from a X Shop (https://blog.twitter.com/en_us/topics/product/2022/twitter-shops-more-space-to-shop):

1. From the X Shop, navigate to the product you wish to report.
2. Long-press on the product tile until the report product button appears.
3. Select **Report product.**
4. Select **Intellectual property violation** if you're reporting a product for issues with intellectual property rights. (https://help.twitter.com/en/rules-and-policies#intellectual-property) You'll need to include the product ID. (https://help.twitter.com/en/using-twitter/tweet-and-moment-url#productid) You can also submit an intellectual property violation directly here (https://help.twitter.com/en/forms/ipi).

   Select **Other violation** if you're reporting a product for a different reason.

How to report specific types of violations

The information below outlines the types of violations you can report to us through our Help Center.

- **Unauthorized trademark use:** Learn more about X's trademark policy and file a report here.
- **Unauthorized use of copyrighted materials:** Learn more about X's copyright policy and file a report here.
- **Sale or promotion of counterfeit goods:** Learn more about X's counterfeit goods policy and file a report here.
- **Privacy policy towards children:** Our Services are not directed to persons under 13. If you become aware that your child has provided us with personal information without your consent, please contact us via our privacy form. Learn more about our policy towards children in our Privacy Policy (https://x.com/en/privacy.html).
- **Child sexual exploitation:** Learn more about our child sexual exploitation policy and file a report here.
- **Pornography:** To report obscene or pornographic images being used in profile photos and/or header photos on X, follow our instructions on reporting sensitive media.
- **Impersonation of an individual or brand:** Learn more about our impersonation policy and file a report here.
- **Private information posted on X:** Learn more about our private information policy and file a report here.
- **Abusive behavior and violent threats:** Learn more about our abusive behavior policy and file a report here.
- **Spam and system abuse:** If you are experiencing a spam or malware issue that's impacting your use of X, file a report here.
- **Violation of X Ads policy:** Learn how to recognize X Ads and the steps you can take to resolve issues without filing a report. Report a X Ad that may be in violation of our policies.

Note: When reporting potential violations of the X Rules and Terms of Service (https://twitter.com/tos) through the Help Center, you may be asked to allow us to share parts of your report with third parties, such as the affected account.

How to report on behalf of someone else

You can report violations on behalf of another person. Refer to the categories and instructions listed above or contact us to submit your report. You can also report

directly from a post or profile (see above section **How to report directly from a post, List, or profile**).

Response timeframe

X acknowledges properly submitted reports within twenty-four hours. Although reports are typically resolved within a few days, resolution times vary and may take thirty days to reach resolution based on factors that are often outside of X's control, such as the need for user input and whether a user chooses to appeal.

Share this article

- English (https://help.x.com/en/rules-and-policies/x-report-violation)
- Español (https://help.x.com/es/rules-and-policies/x-report-violation)
- 日本語 (https://help.x.com/ja/rules-and-policies/x-report-violation)
- 한국어 (https://help.x.com/ko/rules-and-policies/x-report-violation)
- Português (https://help.x.com/pt/rules-and-policies/x-report-violation)
- Deutsch (https://help.x.com/de/rules-and-policies/x-report-violation)
- Türkçe (https://help.x.com/tr/rules-and-policies/x-report-violation)
- Français (https://help.x.com/fr/rules-and-policies/x-report-violation)
- Italiano (https://help.x.com/it/rules-and-policies/x-report-violation)
- العربية (https://help.x.com/ar/rules-and-policies/x-report-violation)
- Nederlands (https://help.x.com/nl/rules-and-policies/x-report-violation)
- Bahasa Indonesia (https://help.x.com/id/rules-and-policies/x-report-violation)
- Русский (https://help.x.com/ru/rules-and-policies/x-report-violation)
- हिंदी (https://help.x.com/hi/rules-and-policies/x-report-violation)
- தமிழ் (https://help.x.com/ta)
- עברית (https://help.x.com/he/rules-and-policies/x-report-violation)
- 简体中文 (https://help.x.com/zh-cn/rules-and-policies/x-report-violation)
- 繁體中文 (https://help.x.com/zh-tw/rules-and-policies/x-report-violation)
- ภาษาไทย (https://help.x.com/th/rules-and-policies/x-report-violation)
- Tiếng Việt (https://help.x.com/vi/rules-and-policies/x-report-violation)
- Melayu (https://help.x.com/ms/rules-and-policies/x-report-violation)
- ইংরেজি (https://help.x.com/bn/rules-and-policies/x-report-violation)
- Filipino (https://help.x.com/fil/rules-and-policies/x-report-violation)
- فارسی (https://help.x.com/fa/rules-and-policies/x-report-violation)
- Dansk (https://help.x.com/da/rules-and-policies/x-report-violation)
- Suomi (https://help.x.com/fi/rules-and-policies/x-report-violation)
- Svenska (https://help.x.com/sv/rules-and-policies/x-report-violation)
- Norsk (https://help.x.com/no/rules-and-policies/x-report-violation)
- Polski (https://help.x.com/pl/rules-and-policies/x-report-violation)
- Magyar (https://help.x.com/hu/rules-and-policies/x-report-violation)
- Română (https://help.x.com/ro/rules-and-policies/x-report-violation)
- Українська (https://help.x.com/uk)
- मराठी (https://help.x.com/mr)
- અંગ્રેજી (https://help.x.com/gu)
- Български (https://help.x.com/bg/rules-and-policies/x-report-violation)
- Català (https://help.x.com/ca)
- Hrvatski (https://help.x.com/hr/rules-and-policies/x-report-violation)
- Српски (https://help.x.com/sr)
- Slovenčina (https://help.x.com/sk/rules-and-policies/x-report-violation)

- ಕನ್ನಡ (https://help.x.com/kn/rules-and-policies/x-report-violation)
- پښتو (https://help.x.com/ps/rules-and-policies/x-report-violation)
- Dari (https://help.x.com/fa-af/rules-and-policies/x-report-violation)
- Oromo (https://help.x.com/om)
- Tigrinya (https://help.x.com/ti)
- English (https://help.x.com/ckb/rules-and-policies/x-report-violation)
- Lietuvių (https://help.x.com/lt/rules-and-policies/x-report-violation)
- Latviešu (https://help.x.com/lv)
- Malti (https://help.x.com/mt/rules-and-policies/x-report-violation)
- Slovenščina (https://help.x.com/sl)
- Gaeilge (https://help.x.com/ga/rules-and-policies/x-report-violation)
- Lus Hmoob (https://help.x.com/hmn/rules-and-policies/x-report-violation)
- Հայերեն (https://help.x.com/hy/rules-and-policies/x-report-violation)
- ខ្មែរ (https://help.x.com/km/rules-and-policies/x-report-violation)

EXHIBIT 21

Website Terms and Conditions of Use and Agency Agreement

Terms & Conditions | Privacy Policy | Copyright Notification | Counter Notification

Last modified January 29, 2025 **[See Changes]**

TERMS AND CONDITIONS OF USE OF WEB SITE

This web site, Rumble.com (the "Rumble Site"), is operated by Rumble Canada Inc. ("Rumble"). Rumble is a user-generated video content agency that provides a video exchange, video hosting platform and video player. Rumble provides access to user-generated videos and other content ("Content") via the Rumble Site, via the Rumble video player application (the "Rumble Player") and otherwise, including through mobile apps and syndication (collectively, the "Rumble Service" or "Platform"), under certain terms and conditions as set forth below. No person under the age of 17 is permitted to use the Rumble Site.

ACCEPTANCE OF THESE TERMS AND CONDITIONS THROUGH USE

By using the Rumble Service, you signify your agreement to all terms, conditions, and notices contained or referenced herein (the "Terms of Use"). Rumble reserves the right, in its discretion, to update or revise the Terms of Use. Please check the Terms of Use periodically for changes. Your use of the Rumble Service subsequent to the posting of any change(s) to the Terms of Use will be deemed your acceptance of such change(s).

RESTRICTION ON USE OF THE CREATORS COMMENTS, LIVE CHAT & FORUM

Rumble may from time to time offer an online forum, live chat and comments for "Creator Discussions" (the "Forum") where users of the Rumble Service and creators of Content may discuss matters pertaining to the Content and/or the Rumble Service. Your participation in Comments or the Forum is entirely voluntary. As participation may occur in real time and therefore you or others may post something to comments or the Forum that has not [illegible], censored or otherwise controlled by Rumble. Notwithstanding the foregoing, Rumble [illegible] the right to monitor messages on Comments and the Forum and to remove messages [illegible]

8. Content or material that exploits children under the age of 18 or posts or discloses any personally identifying information about any person at any age, including but not limited to personally identifying information about children under the age of 18;
9. Content or material promoting or providing instructional information about illegal activities, promoting harm or injury to any group, individual or cruelty to animals including, but not limited to:

    a. Disseminating personal information about another individual for malevolent purposes, including libel, slander, "doxxing", defamation or violation of an individual's right to privacy.

10. Content or material that infringes or encroaches on the rights of others, including, but not limited to, infringement of privacy, publicity rights, and harm to reputation;
11. Any Content or material that contains links to another website where any of the above-described prohibited Content or material is accessible.
12. Any other Content or material that Rumble in its sole, unfettered, and arbitrary discretion, determines is undesirable on the Rumble Service.

Rumble has the sole discretion to decide whether Content or material is permitted on the Rumble Service and any materials submitted to the Rumble Service may be, but is not necessarily, examined by Rumble before it is made available on the Rumble Service. You acknowledge that Rumble has the absolute right (but not the obligation) to prohibit, refuse, delete, move and edit Content and material for any reason, in any manner, at any time, without notice to you.

You should also know that in visiting the Rumble Site or viewing Content via the Rumble Player or otherwise, you may be exposed to materials which you consider to be offensive or inappropriate and you assume the risk and sole responsibility for your exposure to any such Content or material.

To report content that violates our policies, please email moderation@rumble.com

COMPLAINT PROCEDURE

To report Content you believe violates Rumble's policies, please email moderation@rumble.com. Please use the word "Complaint" in the subject line, and include the following information in your email:

3. If your complaint concerns the activities of other users/visitors on the Rumble Site, identify the specific type of inappropriate or offensive behavior engaged in and, insofar as possible, the identity of the offending person.

4. If your complaint concerns particular Content, please provide the URL for the video that is the subject of your complaint, timestamps within the video where the alleged violative Content appears, and the reason for your Complaint.

A customer service representative will endeavour to respond to your email and if, in Rumble's determination, your complaint is a valid one, Rumble will take appropriate actions in its sole discretion, and has no responsibility to at any time report to you as to the status or outcome of its investigation or any actions Rumble has taken as a result.

AGENCY AGREEMENT

If you are a creator of Content submitted to the Rumble Service through your Rumble account, the relationship between you and Rumble is one of principal and agent ("Agency") and is subject to the terms and conditions set out herein which specifically govern this relationship (the "Agency Agreement").

Appointment of Agent. You, as the principal (the "Principal" or "you"), may submit video Content to be published and managed by Rumble as your agent ("Agent") for the purposes of same. By submitting Content to Rumble and by Rumble accepting such Content on the Rumble Service pursuant to either Agency Option "A" or Agency Option "B", as defined below, you are appointing and do hereby appoint Rumble as your exclusive, worldwide, perpetual Agent for such Content, and grant Rumble the exclusive right to distribute, display, reproduce, license, rent, sell, monetize, and otherwise exploit the Content in any medium, on any kind of display device, worldwide, for the duration of the "Term of Agency" as defined below (the "Agency Rights"). As discussed in more detail below, the Agency Rights will also include Rumble's right to bring suit in its own name as plaintiff for infringement or other inappropriate or illegal use of the Content and to seek in such suit all damages or other relief available under law and equity to which you and/or Rumble are entitled. By appointing Rumble as your Agent and granting Rumble the Agency Rights, you agree that you shall not distribute, display, reproduce, license, rent, sell, monetize, and otherwise exploit the Content in any medium, on any kind of display device, worldwide, for the duration of the Agency Term, as defined below. The Agency Term means a 50 (fifty) year period commencing as of the date you enter into this Agreement. The Agency Term shall automatically renew for additional consecutive renewal terms of 50 (fifty) years each, unless either party gives written notice of its intent not to renew the Agency Term, ninety (90) days prior to the expiration of the then expiring Agency Term.

EXHIBIT 22

Terms of Use

Effective Date March 27, 2020

Last Modified: May 1, 2024

Welcome to the website of Babylon Bee, LLC ("**Babylon Bee**," "**Company**," "**us**," or "**we**"). The following terms and conditions, together with any documents they expressly incorporate by reference, including without limitation the Privacy Policy, Privacy Notice for California Residents, and Terms of Online Sales (collectively, these "**Terms of Use**" or "**Terms**"), govern your access to and use of https://babylonbee.com (the "**Company Site**") and as otherwise provided for herein with respect to the Company's social media pages on various third party social media platforms (each a "**Social Media Page**," together with the Company Site, collectively, the "**Site**").

Please read the Terms of Use carefully before you start to use the Site. These Terms contain a binding arbitration clause and a waiver of class action rights. If you do not want to agree to these Terms of Use, you must not access or use the Site.

BY ACCESSING, BROWSING OR USING THE SITE (INCLUDING YOUR SUBMISSION OF INFORMATION TO THIS SITE), YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND AGREED TO BE BOUND BY THESE TERMS OF USE, INCLUDING THE PRIVACY POLICY AND THE PRIVACY NOTICE FOR CALIFORNIA RESIDENTS (WHICH ARE INCORPORATED HEREIN FOR ALL PURPOSES), AND TO COMPLY WITH ALL APPLICABLE UNITED STATES LAWS AND REGULATIONS.

You agree that the Terms of Use, combined with your act of using the Site, have the same legal force and effect as a written contract with your written signature and satisfy any laws that require a writing or signature. You further agree that you will not challenge the validity, enforceability, or admissibility of the Terms of Use on the grounds that it was electronically transmitted or authorized.

Eligibility

This Site is offered and available to users who are 18 years of age or older. By

provided herein.

In order to become a subscriber (by registering for a free or premium account) or to purchase any product or service offered by Babylon Bee we require an individual to be at least 18 years of age. NOTWITHSTANDING, IF YOU ARE UNDER THE AGE OF 18 YEARS OLD OR THE LEGAL AGE OF MAJORITY IN YOUR JURISDICTION OR STATE OF RESIDENCE (EACH, A "**MINOR**"), YOU MAY USE THE SERVICES OR PURCHASE PRODUCTS ON A LIMITED BASIS WITH YOUR PARENT'S OR LEGAL GUARDIAN'S CONSENT; PROVIDED THAT YOUR PARENT OR LEGAL GUARDIAN MUST READ AND CONSENT TO THESE TERMS OF USE. BY PERMITTING A MINOR TO USE THE SERVICES OR PURCHASE PRODUCTS, A MINOR'S PARENT OR LEGAL GUARDIAN (1) BECOMES SUBJECT TO THESE TERMS OF USE, (2) AGREES TO BE RESPONSIBLE FOR THE MINOR'S ACTIVITIES AND INTERACTIONS WITH THE SERVICES OR THE PURCHASE OF THE PRODUCTS, AND (3) ACKNOWLEDGES AND AGREES THAT A MINOR WILL HAVE ACCESS TO LIMITED FEATURES OF THE SITE AND THE SERVICES. It is a violation of these Terms of Use to provide false or misleading information to Babylon Bee in connection with the creation of an account or to make any such purchase or use any of our services. In the event that we discover that a Minor created an account without the proper authorization from the Minor's parent and/or legal guardian (as described herein) on our Site then we will immediately terminate that Minor's account. If you would like to report an unauthorized account registered for a Minor, please contact us at https://babylonbee.com/contact.

Contact Information

Should you have any questions about these Terms of Use, please contact us at:

Babylon Bee
Attn: Customer Service - Privacy
110 Front Street, Suite 300
Jupiter, FL 33458

or

https://babylonbee.com/contact

All notices of copyright infringement claims should be sent to the designated agent set forth below in the section titled, Procedure for Submitting Notification of Alleged Copyright Infringement, in the manner and means set forth therein.

affiliates and licensors. All rights reserved.

Digital Millennium Copyright Act

In the event of an alleged copyright infringement, Babylon Bee shall act expeditiously in accordance with the Digital Millennium Copyright Act ("**DMCA**") (17 U.S.C. § 512) and will take steps to have the allegedly infringing material removed or access to such material blocked.

Procedure for Submitting Notification of Alleged Copyright Infringement

It is our policy to respond to notices of alleged copyright infringement that comply with the DMCA. With respect to copyright infringement, the DMCA requires Babylon Bee to have a designated agent to receive notices of alleged copyright infringement. For any Contents accessible on the Site that you believe infringes your copyright, please send a written notice of alleged copyright infringement to Babylon Bee's designated agent at the following address:

Babylon Bee DMCA Agent
Nason, Yeager, Gerson, Harris & Fumero, P.A.
ATTN: Brian Hickey, Esq.
3001 PGA Blvd, Suite 305
Palm Beach Gardens, FL 33410
Telephone: (561) 686-3307
Email: bhickey@nasonyeager.com

Your written notification of alleged copyright infringement should include all of the following information:

1. Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works are to be covered by a single notification, a representative list of such works;
2. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit Babylon Bee to locate the material on its server;
3. Information reasonably sufficient to permit Babylon Bee to contact you, such as an address, telephone number, and, if available, an email address at which you may be contacted;

5. A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; and
6. Your physical or electronic signature.

Counter Notification Procedures

If you believe that material you posted on the Site was removed or access to it was disabled by mistake or misidentification, you may file a counter notification with us by submitting written notification to our copyright agent designated above. The DMCA allows us to restore the removed content if the party filing the original DMCA notification does not file a court action against you within ten (10) business days of receiving the copy of your counter notification. Pursuant to the DMCA, the counter notification must include substantially the following:

1. An identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access disabled;
2. Adequate information by which we can contact you (including your name, postal address, telephone number, and, if available, email address);
3. A statement under penalty of perjury by you that you have a good faith belief that the material identified above was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled;
4. A statement that you will consent to the jurisdiction of the Federal District Court for the judicial district in which your address is located (or if you reside outside the United States for any judicial district in which the Site may be found) and that you will accept service from the person (or an agent of that person) who provided the Site with the complaint at issue; and
5. Your physical or electronic signature.

Please be aware that if you knowingly materially misrepresent that material or activity on the Site was removed or disabled by mistake or misidentification, you may be held liable for damages (including costs and attorneys' fees) under Section 512(f) of the DMCA.

Procedure for Submitting Notification of Alleged Intellectual Property Infringement (other than copyright infringement)

If you believe that any Contents posted using this Site infringes the intellectual property that you own or are licensed to enforce (other than your copyright),

Your Privacy Rights

All information we collect on this Site is subject to our Privacy Policy and our Privacy Notice for California Residents . By using the Site, you consent to all actions taken by us with respect to your information in compliance with the Privacy Policy and Privacy Notice for California Residents, as applicable.

Linking to the Site and Social Media Features

You may link to our homepage, provided you do so in a way that is fair and legal and does not damage our reputation or take advantage of it, but you must not establish a link in such a way as to suggest any form of association, approval, or endorsement on our part without our express written consent.

This Site may provide certain social media features that enable you to:

- Link from your own or certain third-party websites to certain content on this Site.
- Send emails or other communications with certain content, or links to certain content, on this Site.
- Cause limited portions of content on this Site to be displayed or appear to be displayed on your own or certain third-party websites.

You may use these features solely as they are provided by us, solely with respect to the content they are displayed with, and otherwise in accordance with any additional terms and conditions we provide with respect to such features. Subject to the foregoing, you must not:

- Establish a link from any website that is not owned by you.
- Cause the Site or portions of it to be displayed on, or appear to be displayed by, any other site, for example, framing, deep linking, or in-line linking.
- Link to any part of the Site other than the homepage.
- Otherwise take any action with respect to the materials on this Site that is inconsistent with any other provision of these Terms of Use.

You agree to cooperate with us in causing any unauthorized framing or linking immediately to stop. We reserve the right to withdraw linking permission without notice.

We may disable all or any links at any time without notice in our discretion.